AI Regulatory Fragmentation and MNE Strategy: Evidence from Microsoft, Salesforce, and Oracle

AI Regulatory Fragmentation and MNE Strategy: Evidence from Microsoft, Salesforce, and Oracle

Capstone Project

Bachelor of Arts in International Business

John Cabot University

Grace Sullivan

Fall 2025

Acknowledgements

I would like to express my sincere gratitude to Professor Maria Jell Ojobor, whose guidance and support were essential throughout the development of this capstone project. Her thoughtful feedback, sustained encouragement, and generous investment of time continually pushed this thesis to a higher standard. Her support has had a profound impact on my academic and personal growth. This work would not have been possible without her guidance and stands as a testament to her dedication to her students.

Abstract

This thesis examines how fragmentation in artificial intelligence (AI) regulation affects international business strategy in Software as a Service (SaaS) firms. It compares Microsoft, Salesforce, and Oracle to show how regulatory divergence between the European Union and the United States shapes choices to standardize or adapt data architectures, AI products, and governance. Using a qualitative multiple case design, the study analyzes company reports, technical documentation, and selective secondary sources from 2023–2025. This analysis is done through the theoretical framework of standardization versus adaptation theory and contingency theory. The findings show that all three firms localize data architecture over product features or governance. Microsoft and Salesforce follow hybrid strategies as they keep a global AI product and governance core, while adding EU specific data residency, routing, and controls. Oracle instead follows a fully adapted strategy through an isolated EU sovereign cloud. Across cases, data sensitivity and compliance risk are the main factors that push firms toward hybrid or fully adapted responses, while strong infrastructure control reduces the cost of deeper localization. Overall, the study shows that AI regulatory fragmentation reshapes the standardization vs adaptation trade-off and that hybrid, data centric adaptation is an effective strategy for global SaaS firms under emerging fragmented AI regimes.

Introduction

The international business environment is being reshaped by rapid technological change, regulatory fragmentation, and geopolitical uncertainty. Artificial Intelligence (AI) is a particularly powerful source of disruption. It enables firms to scale knowledge, automate decisions and processes, and personalize services across borders, but it also exposes them to heterogeneous legal, ethical, and societal expectations. Different jurisdictions have contrasting views on how to balance innovation and accountability, and this is producing fragmented regulatory approaches to AI, especially between the United States and the European Union. For international Software-as-a-Service (SaaS) firms that have AI products or features, these differences create a concrete strategic issue: how to design global AI offerings and data infrastructures that can operate efficiently across markets while complying with conflicting regulatory demands.

Existing research in international business shows that environmental volatility and regulatory complexity shape firms' global strategies, including their degree of standardization versus local adaptation. Studies on digital trade and data governance document how privacy and data protection rules constrain cross border data flows, drive data localization, and increase compliance costs. Work on platform and cloud businesses highlights how digital infrastructures can be reconfigured to meet local requirements while preserving global scale. Recent scholarship on AI governance further emphasizes the growing distance between major jurisdictions in terms of risk classifications, liability, and transparency expectations. Together, this literature suggests that AI regulation is becoming an important part of the institutional environment that multinational enterprises (MNEs) must navigate.

However, there seems to be a gap in the existing knowledge. First, most studies focus on data protection and cross border data transfer rules, with less attention to AI specific regulation as a distinct source of fragmentation. Second, prior work tends to examine regulatory impacts at a macro level, such as trade flows or investment patterns, rather than at the level of firms' internal product, data, and governance architectures. Third, there is limited empirical research on how global SaaS firms with AI features actually respond to diverging regulatory regimes in practice, and under what conditions they choose standardization, hybrid approaches, or full adaptation. As a result, there is a gap in knowledge about how AI regulatory fragmentation translates into concrete strategic design choices inside firms.

This study addresses these deficiencies by examining how international SaaS firms strategize their AI related data architectures, products, and governance processes in a fragmented regulatory environment. Focusing on Microsoft, Salesforce, and Oracle, which all provide AI enabled services in both U.S. and European markets, the thesis investigates when and why they standardize or adapt key elements of their AI offerings across borders. Clarifying these choices is important for several audiences. For managers, it offers guidance on designing scalable yet compliant AI services in major jurisdictions. For policymakers, it provides insight into how regulatory divergence shapes firm behavior and investment in digital infrastructure. For scholars, it links emerging AI regulation to core debates on standardization versus adaptation in international business and helps to conceptualize regulatory fragmentation as a strategic constraint for global SaaS firms.

Literature Review

In today's international business environment, firms operate within the context of volatility, technological disruption, and evolving regulation. Rapid advances in AI are reshaping global operations while also generating new governance and compliance challenges. This literature review examines how volatility, AI as a disruptor, and regulatory fragmentation interact to influence MNEs' strategic choices between standardization and adaptation.

Volatility in the Global Business Environment

The international business environment is impacted by rapidly changing dynamics and complexity. Uncertainty shifts demand, technologies, and non-market conditions globally leading to greater environmental dynamism and complexity in international business to heighten information requirements and raise the consequences of strategic decisions (Dess & Beard, 1984; Duncan, 1972). Strategic design often turns on state, effect, and response uncertainty. Executives must understand what is changing, how it affects performance, and which actions will work, each implying different design and governance needs for the MNE (Milliken, 1987). Changes in economic policy and the uncertainty of such are empirically linked to delayed investment and hiring, promoting volatility through global value chains (Baker, Bloom, & Davis, 2016). In volatile environments, international business can benefit through reconfigurable assets and routines. This is key for dynamic capabilities to conduct timely sensing, seizing, and transforming during a period of volatility (Teece, Pisano, & Shuen, 1997). Environmental disruptions for MNEs include cross border fragmentation in regulations, customer expectations, and factor markets leading MNEs to have to decide to standardize or adapt their products, data practices, and governance. Environmental volatility shifts the optimal position on the standardization adaptation spectrum by altering scale economies, coordination costs, and local legitimacy requirements. This paper synthesizes how environmental uncertainty interacts with AI to predict when firms standardize versus adapt.

AI Implications for International Business

Definitions & Capabilities

AI has emerged as a technological force that is both a driver of disruption and a catalyst for organizational transformation. In order to analyze the complexities of AI and its implications for international businesses, definitions and importance must be discussed. To begin, this literature review will define what AI is and its context in the international business environment. AI can be defined as “a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy” (Menzies et al., 2024). A further definition of AI defines it as “the science and engineering of making intelligent machines” (Menzies et al., 2024). Through using these definitions of AI, the context in which AI is used in international business can be further analyzed. The AI capabilities also require further analysis on global scaling while considering local adaptations. AI not only responds to but also creates new forms of volatility.

Strategic Value & International Business Context

Understanding the impact of AI on the international business environment is crucial for further analysis on how regulations can impact international business. According to Menzies, “Artificial intelligence (AI) has emerged as a pivotal force reshaping the international business

(IB) landscape. In an era of digital revolution, AI technologies have become essential tools for enhancing operational efficiency, decision-making, and innovation globally" (Menzies et al., 2024). In the context of international business these capabilities can be applied to foreign market screening, multilingual customer engagement, and supply chain forecasting (Menzies et al., 2024). Furthermore, small and medium enterprises (SMEs) that are using AI and Machine learning (ML) are experiencing enhanced innovation outcomes and processes (Nafizah, Roper, & Mole, 2024). AI can bring significant innovation and optimization to international business processes, making it an important technology for international business to consider. As Trivedi & Gautam note, "the advancement of digital platforms has fundamentally transformed cross-border trade, enabling greater market access, reducing operational costs, and enhancing trade efficiency" (Trivedi & Gautam, 2025). Analyzing and understanding these benefits is important in understanding the overall impact digital regulations have on international business operations.

Frictions in the International Business Environment

AI can bring substantial benefits to international businesses, but it is not without friction. This is a new technology in a rapidly developing landscape, so challenges will arise. A main challenge for international business is operating across borders. Protectionist policies, privacy issues, security issues, lack of AI provisions in trade agreements, and growth and changes in international AI instruments all need to be considered (Menzies et al., 2024). Furthermore, according to Menzies, "access to trained IT professionals and programmers is key for developing AI solutions, and there appear to be barriers to the movement of people across countries with these skills. Lowering these barriers would facilitate the transfer of AI-related knowledge and skills" (Menzies et al., 2024). These barriers and challenges must be examined by international businesses in order to implement AI more effectively. There are various barriers international businesses must navigate when dealing with digital regulation. These can include cybersecurity risks, privacy concerns, and regulatory complexities (Trivedi & Gautam, 2025). Cybersecurity and privacy are major focuses of regulation, making them central concerns. Furthermore, international businesses must correctly and fully understand the regulation in order to ensure compliance which can lead to complexities with interpreting and implementing the standards. Adding to this, the fragmentation of digital regulations makes compliance even more complicated for international businesses as they have to navigate and implement various complex standards in order to ensure operational success.

Challenges of AI: Regulatory Fragmentation Impact on International Business

Context & Importance

While AI can bring transformative opportunities, it presents challenges concerning the divergent regulatory regimes. These differences in data, privacy, and AI governance create a fragmented environment that limits scalability and complicates MNE strategies. The regulatory distance framework describes this through the emphasis of the degree of divergence between AI/data regulations across regions and its impact on cross border data/AI system design (Ghemawat, 2001). Regulations shape how international businesses structure and strategize their actions. It is imperative to understand and follow the various national and international regulations of the markets in which the business operates in order to ensure success and regulatory compliance. Regulatory fragmentation happens when there are different standards of regulation in different markets leading to different sets of rules that an international business will need to ensure they are complying with. This can lead to challenges as an international business must be aware of all these different standards and ensure they are complying with all the regulations in the market they are operating in. AI opportunities coexist with regulatory barriers meaning interoperability and quantity of cross border regulations will determine how efficient a firm will be in generating performance from AI trendlines (Vanessa, 2024).

Data Governance & AI in International Business

In order to fully analyze the impacts of AI regulations on MNEs, the issue of data governance must be discussed. AI operates through using a mass amount of data in order to generate its outcome. Due to this, this paper will analyze data governance and how this shapes regulations of AI. Data has been identified as the primary factor of digitalization and the increase in regulations concerning data has heightened cross border challenges (Coche et al., 2024). Academics discuss data governance and its importance for international business as there are risks from regulatory multiplicity, variance, and incompatibility (Coche et al., 2024). International businesses must be aware of these risks and challenges that come from data governance and how that impacts the regulations on the use and implementation of AI.

The Brussels Effect & Divergent Models

A framework in which the implication of these standards can be analyzed is the Brussels effect. The Brussels effect pertains to the EU's unilateral power to regulate global markets (Coche et al., 2024). This is based on the five conditions of market size, regulatory capacity, political will, inelastic targets, and non-divisibility (Coche et al., 2024). Within the Brussels effect there is de facto and de jure. De facto Brussels effect is when an MNE standardizes internationally in adherence to a single regulation. De jure Brussels effect is when an MNE pressures their home government to adopt the EU regulation in order to avoid competitive disadvantages (Coche et al., 2024). This effect can be seen with the EU's General Data

Protection Regulation (GDPR) as it has seemed to drive global compliance (Coche et al., 2024). According to Coche, “the GDPR regulates how data can be used (i.e., processed) and therefore obliges firms to respect certain principles, such as to be transparent towards their users; to limit data processing to what is strictly necessary; and to ensure that data is accurate and secure” (Coche et al., 2024). The GDPR is an example of a de facto regulation as many MNEs have adopted this standard. The GDPR has also influenced other nations such as Brazil and Australia to mirror the framework of their regulations with similar legislation with Brazil’s Lei Geral de Proteçao de Dados and Australia's Privacy Amendment Act 2017 (Coche et al., 2024).

While the EU standard seems to be globally impactful, there are still other nations enforcing different standards. The three main variations in standards are in the EU, the US, and China. The EU is fundamental rights oriented and is considered conditional, the United States is market and consumer rights oriented and is considered open, and China is national security-oriented while being considered limited (Coche et al., 2024). As defined by the World Development Report, an open model is one where there is no comprehensive data protection framework and data protection is considered a consumer right (Coche et al., 2024). A conditional model is considered the fundamental right approach and there is a preventative framework for data protection (Coche et al., 2024). The limited model is one where data protection is considered a national security issue and allows governments to have broad state control over access to and use of data (Coche et al., 2024). Within the US open model, privacy protection has largely developed through sector specific and state level laws rather than a comprehensive federal framework. A prominent example is California’s Consumer Privacy Act (CCPA), which grants California residents rights to know what personal information is collected about them, request deletion, and opt out of the sale of their data, imposing transparency and governance duties on large data intensive firms (Farhad, 2024). CCPA is built around a narrower, consumer-oriented concept of personal information than the EU's fundamental rights based concept of personal data and excludes categories such as publicly available information, which increases regulatory distance between EU and US regimes (Coche et al., 2024). These definitional and institutional differences mean that, even before AI specific rules, MNEs already face fragmented requirements when designing data and AI architectures across EU and US markets.

Data Transfers & Localization

Data transfers and localization are part of the regulatory concerns MNEs may face with the use of AI. A data transfer refers to the movement of information between systems, whereas data localization refers to the regulatory practice that requires data to be stored and processed within a nation's borders to protect privacy and ensure local regulatory compliance (Coche et al., 2024). Schrems I and II invalidated existing mechanisms for lawful data transfers between the EU and the US, introducing a high threshold for transatlantic data transfers (Coche et al., 2024). The existing mechanisms it invalidated were the Safe Harbor and Privacy Shield. Furthermore, these judgments imposed strict standards on the use of Standard Contractual Clauses, and required firms to ensure data of EU citizens receives essentially equivalent protection of the EU standards (Coche et al., 2024). According to Coche, the European Schrems I and II judgments highlighted a lack of interoperability between regions highlighting the impact of regulatory fragmentation (Coche et al., 2024). These judgments show how the regulatory environment is ever evolving, and it can lead to serious impact on how MNEs have to operate in the regulatory environment. This implication highlights how MNEs may need to implement an adaptation strategy to data pathways even if the main model continues to be standardized.

Furthermore, the use of data and data localization usually is defined by a spectrum. Nations that have a model for cross border data transfers either are classified as open, conditional, or limited based on the models discussed previously for data protections (Coche et al., 2024; López González et al., 2022). With the open classification the company is free to decide how they transfer data to third countries. With the conditional classification ex-ante requirements must be met before data can be transferred. With the limited classification data transfers are prohibited or require government approval. The nations that are considered open are Australia, Mexico, and the US. The nations that are considered conditional are Argentina, the EU, Singapore, and Turkey. The nations that are considered limited are Brunei, China, Russia, and Tunisia (Coche et al., 2024; López González et al., 2022). MNEs must be aware of these regulatory frameworks and understand what laws they must comply with when operating in a variety of markets.

New EU Regime Interactions

The EU has begun to create new regulations that extend beyond personal data and into industrial data which is what powers AI. The EU has enforced a new regulation that further impacts the way MNEs operate concerning digital and AI functions. According to de Elizalde, "The Digital Markets Act lays down harmonized rules for contestable and fair markets where gatekeepers are present to the benefit of business users and end users" (de Elizalde, 2025). However, certain features of this regulation have created challenges for MNEs. One important feature of this new regulation is that only significant market actors are subject to this regulation. The regulation binding these actors together leads to fragmented consumer laws since firms in the same sector of the economy are subject to equal rules (de Elizalde, 2025). Protection under the DMA is for both commercial and non-commercial purposes, meaning that consumers and businesses are treated equally to an extent (de Elizalde, 2025). When looking at all the EU regulatory frameworks together, fragmentation is visible. According to de Elizalde, “The interaction of the DMA and DSA with the GDPR has fragmentation effects on consumer law. It partitions businesses’ obligations based on size and enlarges the beneficiaries of those obligations to reach non-consumers” (de Elizalde, 2025). Furthermore, the DMA is considered lex specialis due to this set of regulations that are applied only to the gatekeepers of the market that overrides the general regulatory scheme of the same objective (de Elizalde, 2025). So, these regulations exist with each other rather than replace them.

Furthermore, the EU has also implemented the Data Act (DA) and the Data Governance Act (DGA). The DGA extends GDPR safeguards to non-personal data transfers leading to barriers for cross border data flows (via Coche et al., 2024). This generates friction for international business and could possibly lead to a Brussels effect situation where other nations are pressured to further develop their trade and IP protections (Heiber & Workman, 2023; Vogelezang, 2022). The DA and DGA together help reshape the EU’s data governance in a new way. The DA enforces Internet of Things (IoT) manufacturers to provide user access to device generated data and to share this data with third parties. This helps generate after markets and innovation but can lead to privacy and trade risks. This is where the DGA supports the regulations by creating processes and structures for trustworthy sharing, neutral data intermediation services, and data altruism mechanisms in order to provide safe data for a wider market of usage (Coche et al., 2024). The DGA allows for sharing of both personal and non-personal data in order to support innovation. However, these regulations have also created a chilling effect where firms refrain from data sharing or transferring across borders because of the uncertainty about whether data sharing aligns with regulation (Coche et al., 2024). The risk of liability if the data transfer actually adheres to the regulations may discourage data flows (Coche et al., 2024). For example, firms may restrict cross border industrial data reuse until the regulatory environment settles further leading to delays in after-market analytics and predictive maintenance offerings (Coche et al., 2024). MNEs need to be aware of the changes in data access rights, transfer conditions, and sharing channels. It is clear that comprehensive and fragmented regulations disrupt the international business environment. There are benefits and challenges to these new regulations, and MNEs must strategize their operations for these fragmented regulations.

EU AI Act

The EU has begun to establish even more specific regulations for AI that move beyond the scope of data. The EU AI Act is a risk-based framework that restricts certain unacceptable risk uses such as social scoring and untargeted facial scraping. It also enforces strict obligations for high-risk AI and general purpose AI (GPAI) models (European Union, 2024). The Act entered into force on August 1, 2024; prohibitions take effect February 2, 2025. GPAI obligations will begin from August 2nd, 2025, and high-risk obligations will begin by 2026-2027 (European Commission, n.d.-a; European Parliamentary Research Service [EPRS], 2025). Serious violations of this act can result in €35 million or 7% of global turnover (European Union, 2024). This concerns MNEs as these AI obligations also interact with GDPR/DA/DGA. The AI Act regulates system design and assurance, and the data laws regulate where data can flow and what data can be processed. These regulations together further complicate the cross border regulatory adherence and will have an impact if firms decide to standardize globally or regionally for their AI and data processes (European Commission, n.d.-b). These layers of digital and AI regulation, often overlapping or inconsistent, mean that MNEs must balance global integration with local compliance. This challenge is reflected in the longstanding strategic debate between standardization versus adaptation strategy. Table 1 summarizes the EU AI regulatory environment below.

EU Instrument	Scope & Relevance	Obligations	Timeline & Penalties	Intersections & Notes
GDPR (Reg. (EU) 2016/679)	Personal data protection with global spillovers.	Lawfulness, transparency, minimization, security; transfer tools	In force since 2018, significant turnover based fines	Interacts with AI Act (training data provenance, purpose limits) and DGA (sharing channels)
Data Governance Act (DGA) (Reg. (EU) 2022/868)	Trust frameworks for sharing including non-personal/public sector data; intermediation; altruism.	Neutral data intermediation; safeguards; extra EU access controls; public sector re-use rules	Adopted 2022; phased application	Extends GDPR style safeguards to non-personal sharing; affects cross border access conditions
Data Act (Reg. (EU) 2023/2854)	Access/use rights for device/IoT-generated data; B2B/B2C sharing duties.	User access/portability; compelled sharing under conditions; safeguards for trade secrets/IP	Adopted 2024 (formal number 2023/2854); staged application 2024–2025+	Complements DGA to open industrial data while managing IP/TS risks
Digital Markets Act (DMA) (Reg. (EU) 2022/1925)	Competition rules for digital gatekeepers.	Self preferencing bans; data use constraints; interoperability duties	In force 2022; compliance tied to designations	Works with DSA/GDPR; obligations vary by firm's platform role/size

Digital Services Act (DSA) (Reg. (EU) 2022/2065)	Online intermediary/content governance.	Risk assessments; transparency; data access to researchers; due diligence tiers	In force 2022; duties rolling since 2023–2024	Pairs with DMA; overlays with GDPR for user data use & disclosures
EU AI Act (Reg. (EU) 2024/1689)	Risk based AI framework covering GPAI and high-risk AI; bans certain uses.	Prohibitions (e.g., social scoring); obligations for high risk systems and GPAI (data governance, documentation, testing, monitoring)	Entered into force Aug 1, 2024; Prohibitions apply Feb 2, 2025; GPAI obligations Aug 2, 2025; High-risk obligations 2026–2027; fines up to €35m or 7% global turnover	Interlocks with GDPR (data), DGA/Data Act (sharing/access), and DMA/DSA (platform duties); requires EU specific assurance layers
CJEU Schrems I/II (C-362/14; C-311/18)	Struck down Safe Harbor and Privacy Shield; raised bar for EU-US transfers.	Essentially equivalent protection	2015; 2020; ongoing EDPB guidance since 2021	Drives adaptation of transfer tooling; often encourages localization/edge designs

Table 1: EU Data & AI Regulations

Standardization versus Adaptation

The increasing volatility of global environments and the rise of AI driven digital transformation heightens the strategic tension between global efficiency and local responsiveness. This aligns with contingency theory which suggests the degree to which MNEs modify AI systems, data management, and governance to local regulations (Lawrence & Lorsch, 1967). This tension is captured in the standardization versus adaptation framework, which provides a lens for analyzing how MNEs navigate regulatory fragmentation and technological change. When businesses operate internationally, they have to strategize through the framework of standardization or adaptation. Under the standardization strategy, firms offer products with the same design globally while adaptation offers products designed to the designated location (Liu & Shi, 2020). This choice is apparent for any market entry procedure. MNEs have a conflicting choice between choosing global product standardization which brings scale, speed, and brand integrity or choosing local adaptation which aligns with local needs, regulations, and usage contexts (Liu & Shi, 2020). The choice between standardization and adaptation is determined by cost saving, enhanced value delivery from adaptation, and the homogeneity of markets (Ryans et al., 2003). Further factors that can impact these decisions are national culture and economies of scale extending this framework to knowledge management (Ang & Massingham, 2007). Many factors determine the standardization or adaptation strategy of choice. Market demand heterogeneity, price elasticity of demand, technology velocity, economies of scale, and global integration motives all influence the choice in strategy (Liu & Shi, 2020). Market heterogeneity calls for adaptation strategies while global integration motives move more towards standardization strategies (Liu & Shi, 2020). Furthermore, a strategy is influenced by conceptual fit with market conditions, local competition, regulation, brand position, and HQ subsidiary mandates (Venaik & Midgley, 2019). Cultural dimensions also play a role in strategy decisions as entry into markets with high uncertainty avoidance performs better through standardization while locations with high power distance may call for an adaptation approach (Ang & Massingham, 2007).

Standardization and adaptation offer different benefits and risks to MNE. Standardization can provide cost benefits but may also lead to suboptimal sales and lower local performance (Liu & Shi, 2020). Adaptation can help maintain global benefits while improving local acceptance, but it can also lead to higher costs and greater complexity (Liu & Shi, 2020). Standardized frameworks may improve speed whereas adapted frameworks may improve market success with locally curated features (Liu & Shi, 2020). Academics also highlight that the real driver for success is not just one strategy, but whether the strategy aligns with internal coherence and external fit (Venaik & Midgley, 2019). MNE Managers must not only decide which strategy to implement but how to implement it and the implications of such. It is important to consider which elements of the market entry should stay standardized and which should be adapted (Venaik & Midgley, 2019). Understanding each strategy is dependent on the context of the market entry and contingencies and an equifinality lens should be used to determine the final strategy choice (Ryans et al., 2003; Venaik & Midgley, 2019). These strategies apply to MNEs utilizing AI as MNEs face the decisions of which components they need to adapt versus standardize.

AI Regulatory Fragmentations: Implications for MNE Strategy

Digital regulatory fragmentation is one of the main challenges for international business. According to Trivedi & Gautam, "regulatory fragmentation poses challenges for businesses operating across multiple jurisdictions. Different countries have varying regulations concerning data protection, e-commerce taxation, and digital payments, creating compliance complexities for international traders" (Trivedi & Gautam, 2025). Regulatory fragmentation is a challenge international business must learn to overcome in order to ensure successful operation. This friction may push for adaptation in data complexities even in standardized models.

AI regulatory fragmentation shapes MNEs utilizing AI standardization and adaptation strategies. The standardization versus adaptation strategies is the main framework in which AI involved MNEs should navigate AI regulatory fragmentation. It is suggested that AI architectures standardize the global model and data policy, and adapt data residency, edge processing, and retraining pipelines based on jurisdiction (Coche et al., 2024; López González et al., 2022). MNEs operating models should standardize governance and adapt local accountability, documentation to risk class, and transfer rules based on the EU AI Act, GDPR, DGA, DA interactions (European Union, 2024; EPRS, 2025; Coche et al., 2024). For entering a market, MNEs should standardize the main features to ensure speed and brand integrity and adapt user data capture, consent flows, and restricted features based on regional requirements and guidance (Coche et al., 2024). Furthermore, training should be standardized, while specialist roles affected by mobility and licensing barriers should be adapted (Menzies et al., 2024).

To further solidify MNEs' strategies, the connection between strategy and action will be analyzed. MNEs may perform better with an adaptation framework of data flows and assurance while maintaining standardized core models when regulatory fragmentation increases (Liu & Shi, 2020; Venaik & Midgley, 2019). When markets are homogeneous, feature consistency should be standardized, but legal heterogeneity is high, and feature consistency should be adapted (Ryans et al., 2003; Ang & Massingham, 2007). Furthermore, standardization of governance can improve compliance speed (European Union, 2024; EPRS, 2025). After analyzing both the benefits and risks of standardization and adaptation, the conclusion is that a mix of strategies for different components of the MNE may be the best option. Operating models that implement both standardization and adaptation of certain key aspects perform better in situations of high fragmentation (Coche et al., 2024; de Elizalde, 2025). In Table 2, the main concepts and frameworks from this literature review are summarized.

Construct	Key Theories	Synthesis	Strategy for MNEs
Environmental Volatility & Digital Fragmentation	Dynamic Capabilities (Teece et al.); Environmental Uncertainty (Duncan; Milliken)	High dynamism/uncertainty raises information needs and shifts the efficient point on the standardization adaptation spectrum.	Standardize sensing/seizing/transforming routines and issue tracking; Adapt market playbooks and release cadences by jurisdiction.
AI Regulatory Fragmentation	Digital Institutionalism (Coche et al.; de Elizalde); "Brussels Effect" (Coche et al); Regulatory Distance (Ghemawat)	Divergent regimes constrain scalability; EU rules often externalize to non EU firms; regulatory distance shapes AI/data design choices.	Standardize core governance and documentation; Adapt assurance depth, risk class mappings, and local interfaces.
Data Governance & Cross Border Data	Data governance in IB (Coche et al.); Transfer & localization models (López González et al.)	Data is a primary digital production factor; incompatibilities and localization rules create frictions/chilling effects on sharing.	Standardize data policy/taxonomy/transfer tooling; Adapt residency, edge processing, and retraining pipelines per regime.
Standardization Strategy	Integration Responsiveness / standardization–adaptation trade-offs (Liu & Shi, 2020; Venaik & Midgley)	Global uniformity improves scale/speed/brand integrity but risks local misfit under legal heterogeneity; equifinality matters.	Standardize core models, governance, and product baselines; deploy global issue taxonomy & KPIs.

Adaptation Strategy	Contingency Theory (Lawrence & Lorsch); Standardize vs Adapt (Liu & Shi; Venaik & Midgley); Knowledge Localization (Ang & Massingham)	Local tailoring raises acceptance/compliance but increases cost/complexity; pays off when heterogeneity is high.	Adapt data capture/consent, restricted features, documentation depth, and deployment sequencing by risk class & law.
Contingency Factors	Contingency Theory (Lawrence & Lorsch); Dynamic Capabilities (Teece et al.); Institutional/Regulatory Distance & Brussels Effect (Ghemawat; Coche et al)	Performance hinges on fit; more uncertainty and distance increase the need for local responsiveness.	Align standardization/adaptation with these factors and build adaptive, locally informed capabilities.
Strategic Outcomes	Performance Theory (Venkatraman & Ramanujam); IB Adaptation–Performance Link (Ryans et al.)	Outcomes reflect the strategy quality: speed to market vs incident rate vs cost; fragmentation rewards hybrid designs.	First apply one global design for models and governance; then, for each country, adapt data flows, user experience, and legal wording to fit local regulation.

Table 2: Literature Review Main Framework Overview

Methodology

Case Analysis

The empirical analysis of this study examines how Software-as-a-Service companies strategize their AI products and features in a fragmented regulatory environment. The objective is to understand in which situations companies choose to standardize versus adapt when experiencing regulatory barriers. This analysis will directly provide insight for this study's research question as it will analyze the impact of AI regulatory fragmentation on international business strategy. Furthermore, this analysis will reveal how AI regulatory fragmentation influences firms' decision to standardize or adapt in data architecture, product/feature design, and governance processes. Through this analysis, this study will further analyze outcomes that may be associated with different strategy decisions. This will be done by collecting data from international SaaS companies that provide AI products or services. Specifically, these companies are based in the United States in order to analyze the fragmentation effect as the United States has less comprehensive AI regulations compared to Europe. The scope of this analysis focuses on comparing how US companies have to strategize when operating in the European market as the regulations are stricter in Europe. This study will not focus on the regulatory fragmentation with China as their regulations are very strict and oftentimes US companies often face significant restrictions and limited market access in China, therefore beyond this study's scope.

Case Selection

The companies chosen for the empirical analysis are Microsoft, Salesforce, and Oracle. These companies are major SaaS companies based in the United States that operate globally and have significant AI products and services. These companies are chosen as they can help the study analyze its objective as they are U.S.-based companies that operate within Europe and have clear AI products and services that require strategization among the regulatory fragmentation. Microsoft is an international software and cloud company (Windows, Microsoft 365, Azure, AI) that was founded in 1975 and is based in the United States. In 2025, the company reports USD 281.7 billion in revenue and employs around 228,000 people (Microsoft Corporation, 2025a; Microsoft Corporation, 2025b). Oracle is a U.S. based SaaS company focusing on enterprise software, databases, and cloud infrastructure and was founded in 1977. In 2025, the company generated USD 57.4 billion in revenue and had around 162,000 employees (Oracle Corporation, 2025a; Oracle Corporation, 2025b). Salesforce is also a U.S. cloud CRM and enterprise applications company that was founded in 1999. In 2025, the company reports USD 37.9 billion in revenue and has around 76,000 employees (Salesforce, Inc., 2025a; Salesforce, Inc., 2025b). The main AI product or service for these companies are Copilot for Microsoft, Einstein for Salesforce, and Oracle's AI Data Platform. The trio varies in product scope (productivity vs CRM vs data/infrastructure led SaaS), customer mix (SME to highly regulated enterprises), and stack control (application layers vs infrastructure integrated solutions), offering comprehensive insight on how regulatory fragmentation shapes strategy. These are large multinational companies that work directly with data and AI, therefore, the analysis of these companies' strategies can help this study better understand how international businesses strategize in a fragmented regulatory environment. Table 3 provides a descriptive overview of each company. Furthermore, Table 4 summarizes the key components of the empirical analysis.

Company Name	Headquarters	Industry	Core Markets	AI product/Service	Relevant Regulations
Microsoft	Redmond, Washington, USA	IT, SaaS	Cloud computing and enterprise services (Microsoft Azure), productivity & business software (Microsoft 365, Office applications), operating systems, and industry specific cloud + AI solutions via Industry Clouds offering	Copilot	GDPR, DGA, DA, DMA, DSA, EU AI Act, CCPA
Salesforce	San Francisco, California, USA	Cloud software, SaaS	CRM solutions, cloud infrastructure & platforms aimed at business users, industry specific vertical solutions	Einstein	GDPR, DGA, DA, DMA, DSA, EU AI Act, CCPA
Oracle	Austin, Texas, USA	Enterprise software, cloud computing, database management, IaaS, SaaS	Enterprise database systems, data management, SaaS platforms, cloud infrastructure and platform services, enterprise applications: ERP, HCM, SCM, CX, across large organisations, industry specific solutions	Oracle AI Data Platform/ OCI GenAI	GDPR, DGA, DA, DMA, DSA, EU AI Act, CCPA

Table 3: Case Company Overview

Item	Summary
Objective	Examine how SaaS companies strategize their AI products and features in a fragmented regulatory environment, identifying when they standardize vs. adapt in response to regulatory barriers.
Research Contribution	Directly informs the research question by analyzing the impact of AI regulatory fragmentation on international business strategy and revealing how it shapes choices in data architecture, product/feature design, and governance processes.
Unit of Analysis	International SaaS companies (and their AI products/features).
Case Selection Rationale	US globally operating SaaS companies with AI products/services and active EU presence, relevant for observing strategies under stricter EU regulation vs. the US.
Cases (Firms)	Microsoft, Salesforce, Oracle.
Focal AI Offerings	Microsoft Copilot, Salesforce Einstein, Oracle AI Data Platform.
Geographic Scope	Compare US (less comprehensive AI regulation) vs Europe (stricter regulations).
What Standardize vs Adapt Looks At	Whether offerings/features/structure are kept uniform across regions vs modified for EU constraints.
Expected Outcomes	Identify situations that trigger standardization vs adaptation and associated outcomes of those choices across the three domains.

Table 4: Empirical Summary

Data Use & Selection

The data collected are used to analyze how Microsoft, Salesforce, and Oracle strategized in terms of data architecture, AI product design, and governance. The data is also used to analyze how these strategies vary between the US and EU markets and explore the outcomes of each strategy. The data is collected to reflect the firm, product, and region and the impact on process and strategy. The data collected is within the timeframe of 2023-2025 in order to capture the impact of AI regulation. AI and the regulation of it became prominent in 2023 and has grown since then, therefore making 2023-2025 an appropriate time window for the collection of the data.

Data Sources

The data collected were collected from both credible and relevant primary and secondary sources. The majority of the data came from primary sources, so directly from the company's website or publishings. These company-published materials are well suited to this analysis because they formalize how firms publicly commit to data architectures, AI product behavior, and governance arrangements in order to satisfy regulators, reassure enterprise customers, and signal strategy to investors. In doing so, they capture the codified, intentional side of strategic response to AI regulation, which is the focus of this study. These data sources included product admin documents, trust and privacy centers, product release notes, roadmaps, service availability documents, admin UI observations, security and compliance documents, and corporate filings. Secondary sources such as credible tech press or analyst notes were only used when the information could not be directly found from the firms' sources. The priority was always sourced directly from the firms in order to understand their strategic choices and secondary information was used mostly for context or supplementary purposes.

Theoretical Framework

The analysis follows a theoretical framework using the standardization versus adaptation framework, contingency theory, and performance theory. The standardization versus adaptation framework is used to capture the basic strategic choice between keeping AI architectures, product features, and governance uniform across markets or tailoring them to local conditions.

Contingency theory is used to explain how external and internal factors, such as regulatory stringency, data sensitivity, market importance, and resource configurations, shift the efficient point for standardization vs adaptation strategy. Performance theory connects the strategic choices to outcomes such as speed to market, compliance risk, and longer-term market performance. Bringing these theories together, the framework conceptualizes the four core ideas of standardization strategy, adaptation strategy, contingency factors, and strategic outcomes. These constructs structure the analysis and guide the coding scheme described in this chapter, providing a consistent lens for interpreting how firms respond to AI regulatory fragmentation across data architecture, AI products, and governance. Table 5 summarizes this theoretical framework below.

Construct	Theoretical Basis	Definition/Indicators
Standardization Strategy	Standardization vs. Adaptation Theory (Liu & Shi; Venaik & Midgley)	Degree to which MNEs maintain uniform AI architecture, product features, and governance globally. Indicators: unified AI model architectures, global feature parity, centralized governance, standardized data policy statements.
Adaptation Strategy	Standardization vs. Adaptation Theory (Liu & Shi; Venaik & Midgley); Knowledge Localization Theory (Ang & Massingham); Contingency Theory (Lawrence & Lorsch)	Degree to which MNEs modify AI systems, data management, and governance to local regulations. Indicators: localized data centers, region-specific model retraining, jurisdictional compliance variants (EU vs. US), differentiated consent and privacy flows.

Contingency Factors	Contingency Theory (Lawrence & Lorsch); Dynamic Capabilities (Teece et al.); Institutional/Regulatory Distance & Brussels Effect (Coche et al); Knowledge Localization (Ang & Massingham)	External and internal conditions that shift the efficient point on the standardization vs adaptation spectrum by altering information processing requirements, compliance exposure, and reconfiguration capacity.
Strategic Outcome	Performance Theory (Venkatraman & Ramanujam); IB Adaptation Performance Link (Ryans et al.)	Observable results of standardization/adaptation mix. Indicators: Speed-to-market, compliance incidents, operational cost proxies, market performance proxies.

Table 5: Theoretical Framework

Data Collection

Data is collected by firm, product, and region of operation. The primary sources were analyzed in order to extract the relevant data for the analysis. This data was then codified and organized into the tables to enhance visualization. To analyze which strategy the firm employed for each aspect of operation, standardization was coded as S, hybrid was coded as H, and adapted was coded as A. For the contingencies impacting potential strategy decisions, data sensitivity, market criticality, and compliance risk are coded as low, medium, or high to measure the levels of each. To analyze the outcomes of the strategy, speed to market was coded with the US being the baseline compared to an observed lag in release, cost proxy was coded as yes or no depending on if it was present or not, and performance proxy was coded as either strong or growing. Table 7 presents data on data architecture (type of data construct), AI products and features (rollouts and availability), data governance (regulatory framework), and the determined strategy for each. Table 8 presents data on data sensitivity, market criticality, compliance risk, resource availability (the firms' investment abilities), and strategy chosen. Table 9 presents data on the product's speed to market (indicating if there was a lag in the EU release), the cost proxy (an estimated measure indicating if extra costs/efforts were likely involved), compliance incidents (if there were any violations of regulations for the product), and a performance proxy (an estimated measure indicating the adoption and use of the products). Table 6 provides an overview of the data collection below.

Item	Summary
Purpose	Observe when/why firms standardize vs adapt AI across data architecture, product/features, and governance, and link choices to outcomes (speed, cost, incidents, adoption).
Cases	U.S. headquartered SaaS multinationals operating in the EU (Microsoft (Copilot for M365), Salesforce (Einstein/Agentforce), Oracle (AI Data Platform))
Geographies	U.S. vs EU
Timeframe	2023–2025 (captures major AI feature launches and the EU AI Act transition period)
Primary data sources	Vendor trust, privacy & residency docs, admin/setup documents, availability & release notes, admin UI observations, security & compliance documents, financial filings.
Secondary data sources	Reputable tech press & analyst notes for rollout exceptions or adoption indicators.

Table 6: Data Collection Overview

Findings

The data analysis is done through 3 stages: first the type of strategy the firm utilizes is measured, then further factors that influence strategy are analyzed, and finally the outcome of each strategy choice is analyzed. Through this analysis, this study is able to better understand where International SaaS firms with AI Products choose to standardize or adapt, what might further influence this choice, and the outcomes of the strategy.

Standardization versus Adaptation

Codebook

- Standardized = S: Same architecture/feature/governance globally
- Hybrid = H: Global core with regional overlays (EU residency option, EU-only defaults)
- Adapt = A: Material regional differences (sovereign realm, withheld/altered features, separate operations)

Company Name	Data Architecture	AI product/features	Governance
Microsoft	H	H	H
Salesforce	A	H	H
Oracle	A	A	A

Table 7: Standardization versus Adaptation

Microsoft

In Table 7, the firms' strategy is determined for data architecture, AI product, and governance. In terms of data architecture, Microsoft stores and processes Microsoft 365 personal data within the EU for EU customers. EU traffic for Copilot stays inside the EU data boundary (Microsoft, 2025e). Furthermore, admins can set a preferred data location so that a user's data can be migrated into a specific geography. They also have advanced data residency which keeps key data stored in local data centers, prioritizing user migration (Microsoft, 2024c, 2025a, 2025c). Microsoft 365 operates on a global core with regional controls. Therefore, the data architecture strategy is hybrid, as there is a standard core with EU residency options. This means that EU customers can choose to store their data within the EU data boundaries. While Microsoft provides regional data residency options, it does not operate fully isolated regional clouds. Instead, Microsoft 365 runs on a unified global cloud architecture, with customer data stored in region specific locations when required.

For the AI product of Copilot, core features are global but availability, traffic routing, and certain defaults differ from EU users under the EU regulations. The EU processing and localization stay inside the EU and some feature rollouts behave differently in the EU (Microsoft, 2025b; TechRadar Pro, 2025). The US experiences the standard and sees fewer rollout changes and the traffic is processed on a global level (Microsoft, 2025b, 2025d). Therefore, product strategy is considered hybrid as it is not completely localized per region, but the EU customers' traffic and features are adapted to follow the regulations.

For governance, Copilot adheres to privacy and compliance obligations to ensure data residency (Microsoft, 2025b). Furthermore, through the EU Data Boundary program, Microsoft has relocated operational and support processing into EU datacenters and applied EU specific governance controls to ensure that all Microsoft controlled processing remains within the EU (Microsoft, 2024b). Governance is global by design with the same trust and oversight toolset, but it has EU specific controls in order to satisfy EU data boundary and EU AI regulations. Therefore, the governance strategy is hybrid with the US following the global baseline controls and the EU having boundary constrained processing and stricter localization of operational data.

Salesforce

For the data architecture, Salesforce uses the Hyperforce EU Operating Zone, a dedicated EU-only deployment environment that keeps customer data storage, processing, and operational access entirely within the EU. This zone provides EU specific routing and governance controls, ensuring compliance with EU regulations. The data is also stored locally within each country through Hyperforce (Salesforce, 2025b, 2025e). The Salesforce platform operates on Hyperforce with EU adaptations. EU customers can have their data stored and processed entirely within the Hyperforce EU Operating Zone, whereas US customers run on standard Hyperforce regions without these EU only constraints. This creates a materially different regional architecture, so the data strategy is classified as adaptation.

In terms of AI product features, region and language support is available by region, LLM requests are routed across availability zones and processed by the servers closest to the customer's Salesforce region, so AI inference runs near the tenant's deployment and the platform updates monthly with staggered rollouts based on the region (Salesforce, 2025c, 2025d; Salesforce Release Notes, 2025). Einstein's AI capabilities are built as a single global platform, but the way prompts are routed to LLMs and how the resulting data is stored and processed differs by region, in order to meet local residency and regulatory requirements. EU customers experience EU routing aligned within the EU operating zone, while US customers experience global routing and availability, therefore this strategy is hybrid.

For governance, Salesforce follows responsible AI principles, has an AI acceptable use policy, model cards and transparency, and is aligned with the EU AI Act for responsible deployment (Salesforce, 2025a, 2025c; Salesforce Blog, 2020). There is a global governance baseline with regional overlays for the EU. EU customers experience governance tuned for the EU regulations and US customers follow the global baseline, therefore this strategy is hybrid.

Oracle

For data architecture, Oracle operates its EU Sovereign Cloud through EU-based legal entities with EU resident staff and restricted administrative access. This sovereign environment does not share infrastructure with Oracle's commercial EU regions and is not directly connected to other Oracle cloud regions, creating a physically and logically separate EU realm. Regions are independent and resources are based on the region (Oracle, 2024, 2025a, 2025d). There is a distinct EU realm with the EU Sovereign Cloud containing isolated infrastructure beyond resident toggles. EU customers can confine data within this realm and US customers' data operates within the commercial regions (Oracle, 2025a). The strategy for this is adaptation as Oracle operates within a separate EU realm for EU customers.

For AI product features, the feature availability varies by region with Oracle Cloud Infrastructure generative AI not being offered in every commercial region (Oracle, 2025d). This means that Oracle launches Oracle Cloud Infrastructure (OCI) Generative AI first in its US and commercial regions, while a separate, compliant version becomes available later in the EU Sovereign Cloud. Because OCI GenAI is released on a region-by-region basis and includes EU-specific localization, such as EU only inference endpoints, EU resident operations, and modified data processing rules, the EU deployment operates differently from the US version. These regional differences in timing and architecture produce a materially adapted EU implementation. (Oracle, 2025c, 2025d). EU customers can use GenAI inside the EU sovereign realm and US customers experienced earlier and broader access to these features. Therefore, the strategy for this is adaptation.

In terms of governance, it is built into products, and it varies by the regulation of the region. There is a separate governance for EU operations indicating regional adaptation. EU deployments have EU specific controls and US operations follow commercial/regional governance (Oracle, 2025a, 2025b). The strategy for this is adaptation as they have EU specific governance procedures that are separate from those in the US.

Factors that Shape Strategy

Codebook

- Data sensitivity: Low (metadata only), Medium (some user/business data), High (sensitive company and customer data)
- Market criticality: Low/Medium/High based on investments & customer base
- Compliance risk: Low/Medium/high based on intensity and comprehensiveness of regulations
- Resource availability: Weak/Moderate/Strong based on company size and spending ability

Firm	**Product**	**Region**	**Data Sensitivity**	**Market Criticality**	**Compliance Risk**	**Resource Availability**	**Strategy**
Microsoft	Copilot of Microsoft 365	EU	High	High	High	Strong	Hybrid
Microsoft	Copilot of Microsoft 365	US	High	High	Medium	Strong	Hybrid
Salesforce	Einstein	EU	High	High	High	Strong	Hybrid
Salesforce	Einstein	US	High	High	Medium	Strong	Hybrid
Oracle	AI Data Platform	EU	High	High	High	Strong	Adapted
Oracle	AI Data Platform	US	High	High	Medium/ High	Strong	Adapted

Table 8: Factors Impacting Strategy

Microsoft: EU vs US

In Table 8, the factors that impact the firms' strategy are visualized. For the EU, data sensitivity is high, as Copilot is based on M365 user content and prompts and is constrained by the EU data boundary for customer data. Organizations often use M365, so Copilot deals with sensitive and private data (Microsoft, n.d., 2025b, 2025e). Market criticality is high because Microsoft has made substantial EU-specific infrastructure and compliance investments, such as launching the EU Data Boundary across Microsoft 365 and expanding EU cloud regions, indicating the strategic importance of the EU market. Compliance risk is also high, as Microsoft must comply with the GDPR and prepare for the phased rollout of the EU AI Act through 2026–2027, requiring ongoing adaptation to remain compliant in a tightening regulatory environment (Microsoft, 2025e). Resource availability is strong, as FY2025 experienced record revenue of USD 281.7 billion, indicating the capacity to fund compliance initiatives (Microsoft Corporation, 2025a, 2025b). The strategy choice overall was hybrid with a global core and EU data boundary processing and residency controls. This strategy protects sensitive user data and addresses EU compliance risk while retaining a global product core.

For the US, data sensitivity is high due to Copilot operating off of private and sensitive M365 data, and therefore needs to be handled carefully (Microsoft, 2025b). Market criticality is high, as the US is Microsoft's largest and home market, therefore being the Copilot target base (Microsoft, 2024a). Compliance risk is medium as US AI and privacy laws are less comprehensive than in the EU (Microsoft Trust Center, n.d.). Resource availability is strong for the same reasons as above, with profitability to support controls. The strategy is hybrid for the same reason as above as they operate on a global Copilot core with processing varying across regions. The underlying data is highly sensitive, but the lower regulatory pressure in the US compared to the EU allows Microsoft to maintain a largely standardized Copilot product and governance model, with only limited adaptations in how data is processed across regions.

Salesforce: EU vs US

For the EU, data sensitivity is high, as it deals with customer records, messages, files, prompts, and private company information (Salesforce, 2025c). Market criticality is high, as Europe accounts for USD 8.9 billion of Salesforce's USD 37.9 billion in FY2025 revenue, around 24% of total revenue, making it the company's second largest region after the Americas (Salesforce, 2025a, 2025b). The compliance risk is high due to GDPR and the evolving EU AI Act obligations with strong customer demands for regional processing (Salesforce, 2025e). Salesforce has the financial and technical capacity to localize its services, and its prior investment in the Hyperforce platform gives it the infrastructure needed to implement EU specific adaptations. The strategy chosen is hybrid as Hyperforce EU Operating Zone and regional routing keep sensitive data processing within the EU while retaining a global product core.

For the US, data sensitivity is high for the same reason as above, as the platform deals with highly private data. Market criticality is high because the US is the company's home market, representing its primary launch base, a large installed customer base, and a key source of revenue and reputation. Compliance risk is medium as there are fewer comprehensive AI and privacy regulations compared to the EU, and governance is handled on a global scale (Salesforce, 2025a). The resource abilities are strong for the same reasons as above. The overall strategy is hybrid, and the company maintains the standardized Einstein core with enterprise controls and flexible routing.

Oracle: EU vs US

For the EU, data sensitivity is high as enterprise and regulated data is used for AI and analytics (Oracle, 2025b). Market criticality is high, as Oracle is investing USD 3 billion over five years in cloud infrastructure in Germany and the Netherlands, and its EU Sovereign Cloud offering spans all 27 EU member states, indicating that the EU enterprise and government customer base is strategically important (Oracle, 2025a; TelecomTV, 2024). The compliance risk is high with the GDPR and EU AI Act and strong customer demand for EU localized processing. Resource availability is strong with a large OCI regional adaptation efforts and EU specific investments (Oracle, 2025a). The strategy is adaptation as Oracle offers the EU Sovereign Cloud, which is physically isolated with EU operations and separate governance, leading to material regional differences (Oracle, 2024).

For the US, data sensitivity is high for the same reasons as above, as it deals with private company data for AI and analytics. Market criticality is high as it is the core commercial and public sector market for the company. Compliance risk is medium at the aggregate U.S. level, given the fragmented, sector specific AI and privacy regulation rather than a horizontal regime, but rises to high in sectors such as healthcare and the public sector, where regulated entities must comply with HIPAA, medical device rules and state AI specific requirements (HIPAA Journal, 2024; GDPR Local, 2025). Resource availability is strong, supported by Oracle's USD 57.4 billion in 2025 revenue and significant free cash flow, giving the company the financial capacity to fund region specific deployments such as the EU Sovereign Cloud (Oracle Corporation, 2025a, 2025b). The strategy observed is adaptation, as it includes region and sector specific rules and governance, producing materially different deployments for each region (Oracle, 2025c, 2025d).

Strategy Outcomes

Codebook

- Speed to market: US is the baseline (home market); EU is considered staggered if the product was released after its release in the baseline market
- Cost proxy: Any additional required cost or operational effort beyond the normal product licensing. Y if residency, sovereignty, migration, compliance, product adaptation, or extra governance add cost/effort beyond standard licensing
- Compliance Incidents: If a product specific compliance violation has occurred
- Performance: Strong if the product has high adoption and consistent usage within the region; Growing if the product shows increasing adoption and usage but has not yet reached widespread or mature uptake

Firm	Product	Region	Speed to Market	Cost	Compliance Incidents	Performance	Strategy
Microsoft	Copilot of Microsoft 365	EU	Staggered	Y	None	Growing	Hybrid
Microsoft	Copilot of Microsoft 365	US	Baseline	Y	None	Strong	Hybrid
Salesforce	Einstein	EU	Staggered	Y	None	Growing	Hybrid
Salesforce	Einstein	US	Baseline	Y	None	Strong	Hybrid
Oracle	AI Data Platform	EU	Staggered	Y	None	Growing	Adapted
Oracle	AI Data Platform	US	Baseline	Y	None	Strong	Adapted

Table 9: Strategy Outcomes

Microsoft: US vs EU

In Table 9, the outcome of each firm strategy is analyzed. For the US, the speed to market is considered the baseline as this is the home market. Any new Copilot feature is first released in the US (Microsoft, 2025d; Microsoft Tech Community, 2025). The cost proxy is present due to Copilot's additional per user licensing requirements, and the extra security, configuration, and administrative work needed for deployment, which go beyond standard Microsoft 365 licensing (Microsoft, n.d.). There have been no compliance incidents specifically tied to Copilot. The performance has been strong, with early adoption reflected in Microsoft's disclosure that nearly 70% of the Fortune 500 now use Microsoft 365 Copilot and 40% of the Fortune 100 participated in the Early Access Program, indicating high usage and acceptance among large enterprises (Kumar, 2024; Shaw, 2024).

For the EU, the speed to market is staggered compared to the US due to data residency, localization, and EU specific rollout executions (Microsoft, 2025e; TechRadar Pro, 2025). The cost proxy is present with extra cost and efforts related to EU data boundary operations, localization and support with add ons, extra administration and testing burdens. Cost is associated with dedicated EU support, testing, and compliance review (Microsoft, 2025a, 2025c, 2025e). There have been no public incidents specific to Copilot, but it is under ongoing regulatory scrutiny as the AI Act implementation begins to affect Copilot (Microsoft, 2025b, 2025e). The performance in the EU is growing as Microsoft positions the EU Data Boundary as a multi-phase initiative to keep EU customer data stored and processed within the EU/EFTA and notes that additional services and capabilities are being brought in scope over time (Microsoft, 2025e). This expansion is particularly relevant for regulated sectors that require strict data residency, so adoption is expected to increase as more workloads become boundary compliant.

Salesforce: US vs EU

For the US, the speed to market is immediate, as this is the baseline market. All Einstein features and updates tend to be first released in the US market (Salesforce Release Notes, 2025). The cost proxy is present with costs associated with per-user and add-ons for Einstein, noting configuration, change management, and prompt safety guardrails (Salesforce, 2025c). There have been no specific Einstein compliance incidents reported. The performance is coded as strong, as Salesforce reports more than 1,000 paid Agentforce deals, indicating substantial early commercial uptake of its AI platform across core clouds (Reuters, 2024).

For the EU, the speed to market is staggered compared to the US for certain capabilities like language coverage, LLM routing, and agent features due to the reliance on the EU Operating

Zone (Salesforce, 2025d, 2025e). The cost proxy is present with incremental costs from Hyperforce EU Operating Zone, data residency validation, extra administration efforts for region specific testing, and further compliance review (Salesforce, 2025b, 2025e). There have been no compliance incidents linked to Einstein. The performance is growing as Salesforce notes that the Hyperforce EU Operating Zone was created to meet the strict data residency and regulatory requirements of EU organizations, particularly in highly regulated sectors. Because the EU Operating Zone provides EU-only storage, processing, and access controls, Salesforce positions it as an enabler for organizations that require verified data residency before adopting cloud and AI capabilities. This indicates that adoption increases as these controls become available.

Oracle: EU vs US

For the US, the speed to market is immediate as this is the baseline market and new OCI features are often first released in the US market. The cost proxy is present with costs associated with standard regional pricing and enterprise security and governance enablement (Oracle, 2025d). There has been no compliance incident specific to OCI GenAI. The performance is coded as strong, reflecting that Oracle's OCI Generative AI Service is designed to support enterprise data and analytics workloads, including hosting custom models, embedding analytics, and integrating with the Oracle Analytics and Data Intelligence platforms, which suggests the foundation is in place and momentum is building (Oracle, 2025d).

For the EU, the speed to market is staggered compared to the US as there are later services released in the EU commercial regions and the EU Sovereign Cloud endpoints. The sovereign aspect can create additional lag (Oracle, 2025c). The cost proxy is present with incremental costs for EU Sovereign Cloud, migration expenses, and additional compliance review (Oracle, 2024, 2025a). There has been no compliance incident linked to OCI GenAI. The performance in the EU is growing as Oracle positions the EU Sovereign Cloud specifically for public sector and highly regulated industries that require strict EU data residency, EU resident operations, and isolated infrastructure. The offering is explicitly designed to allow these customers to adopt Oracle cloud and AI services under sovereignty constraints, indicating that EU uptake is expected to expand as these sectors leverage the sovereign environment. Figure 1 provides a visual overview of the empirical findings.

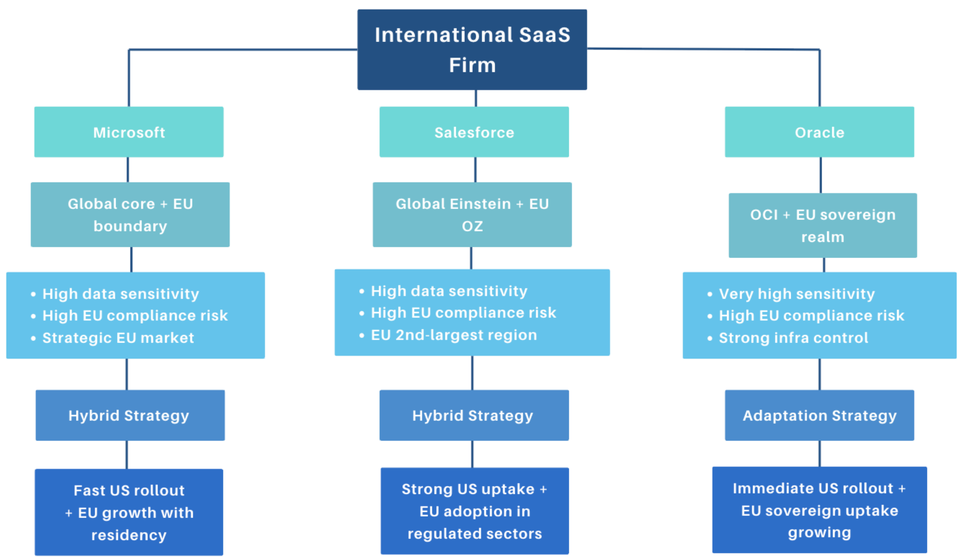

Figure 1: Empirical Findings

Discussion

Across all three companies, EU deployments of products lead to more localization in data architecture compared to feature design or governance. Microsoft and Salesforce retain a global product core and layer EU specific controls and routing, indicating a hybrid strategy. Oracle operates with a materially separate EU realm, showing an adaptation strategy. The outcomes show that releases to the EU market are staggered compared to the US, cost proxies are present where sovereign options are used, no compliance incidents have been observed for any of the products, and adoption is strongest where residency assurances match sector sensitivity.

The findings are consistent with the standardization versus adaptation theory as the cases show firms maintaining a global product core while localizing the data architecture first. This outcome is expected because regulatory pressure forces firms to localize data and operations, but they maintain a global feature layer where standardization delivers the greatest cost and efficiency benefits. The results of hybrid strategies for Microsoft and Salesforce and adaptation for Oracle link to contingency theory. Companies exposed to higher data sensitivity and compliance risk are more likely to adapt in specific components of their architecture and governance. Resource availability supports rather than determines adaptation, and control over infrastructure lowers the cost of localization. Control over infrastructure lowers the cost of localization because firms that own and operate their full cloud stack can deploy region-specific environments, controls, and routing without relying on third-party cloud providers. This reduces the engineering, compliance, and operational costs associated with establishing isolated regions such as sovereign clouds, making deeper adaptation more economically feasible. This is why Oracle adopts a full adaptation strategy as it is more feasible given its strong control over their infrastructure. The outcomes also connect with the theory as greater adaptation correlates with a greater EU release lag and added costs. Hybrid and adaptation strategies help prevent compliance violations and support better performance in sectors that depend on strict data-residency guarantees. This reinforces the theoretical expectation that mixed strategies outperform full standardization in fragmented regulatory environments, and that contextual factors shape the degree of adaptation required.

Data sensitivity and compliance risk are the primary contingencies shaping the firms' strategy. Where compliance risk and data sensitivity are high, firms move to either a hybrid or adaptation strategy. This highlights that higher local regulatory consideration increases local responsiveness. Resource availability enables but does not determine adaptation. All three companies have strong resource availability but only Oracle consistently employs the adaptation strategy. Resource availability is a moderator while regulatory design and product architecture set direction of the strategy. Market criticality moves investment intensity, but not necessarily strategy. The EU strategic importance explains the EU options for Microsoft and Salesforce, but they both still prefer a hybrid strategy where they can preserve a single global feature set. Oracle's control over infrastructure lowers the cost of sovereignty making the adaptation strategy feasible without fragmenting the product portfolio. Data architecture often adapts first, then governance, and finally product/feature design. Firms will localize where they need to comply with strict regulations and keep global uniformity where customer experience and economies of scale are highest, and then shift processes to connect them.

There are certain outcome tradeoffs for each strategy mix. Increased adaptation correlates with greater EU lag, especially with sovereign cloud environments. Adaptation raises operational and migration costs, while a hybrid strategy can lessen the costs by reusing the global core. Hybrid and adaptation strategies can reduce compliance risk as no incidents have been reported for any of the products. Hybrid strategies sustain fast adoption in the US while adaptation strategies improve EU adoption in regulated sectors by clearing regulation barriers.

In international SaaS companies deploying AI products, the efficient strategy is hybrid by having a global core and adapting where the regulations require. Firms minimize fragmentation by holding the feature layer constant and shifting localization into data architecture and residency options. Adaptation is only necessary when regulations require isolated realms or sector constraints. This works for Oracle as it has tighter infrastructure control in order to implement the adaptation strategy feasibly.

Implications

This study builds on the literature of international business strategy specifically within fragmented regulatory environments. This is done by illustrating how AI regulatory fragmentation influences firms' standardization versus adaptation strategy. This study finds that under regulatory fragmentation, firms prioritize data architecture localization while maintaining global product and governance cores. This demonstrates that adaptation strategies can be selective across technical and organizational dimensions rather than a complete adaptation of all processes. The results further confirm contingency theory framework with regulatory pressures and data sensitivity acting as main contingencies while resource availability supports rather than determines strategic outcomes. Furthermore, the study also supports performance theory with compliance to regulations enhancing long term performance.

For international business managers, the findings suggest that hybrid strategies provide the most efficient balance between scalability and local adoption. This means maintaining a standardized AI product core with regional data and compliance overlays. Firms should invest in data architectures and governance frameworks in order to adapt to regional regulations without fragmenting global product development. Managers should also view compliance as an input, meaning that aligning early with regional regulations can accelerate adoption in regulated industries and help firms prepare for future market restrictions. Therefore, managers should prioritize flexible infrastructure, compliance approaches, and dedicated regional oversight to maintain competitiveness in strict AI regulatory environments.

For regulators, the findings highlight the importance of interoperability and regulatory clarity. Fragmented regulatory environments lead to localization strategies that can increase operation costs and potentially slow innovation. Harmonizing AI and data regulatory standards can reduce inefficiencies while maintaining privacy and safety. Regulators may benefit from creating cross border frameworks to reduce compliance duplications for international firms.

Limitations

This study provides important insight into how international SaaS firms strategize their AI operations in a fragmented regulatory environment, however, several limitations should be acknowledged. The first limitation is based on the scope and case selection. The analysis focuses only on three major U.S. based SaaS companies with European operations. These firms are large multinational corporations, and their scale and resources may not reflect strategic realities for smaller or regionally constrained firms. The findings cannot be generalized to all SaaS providers or to firms operating on a smaller scale. Furthermore, the comparison is limited to the U.S. and the EU. Other significant jurisdictions such as China, Canada, or other international AI regulatory frameworks were excluded due to limited data availability and varying market restrictions. As a result, this study mainly focuses on the fragmentation between two jurisdictions rather than a complete global view. The next limitation is based on time constraints as the data only covers the time frame of 2023-2025, capturing the emergence and early implementation of the EU AI Act but not its full enforcement. The regulatory environments concerning AI will continue to evolve and future developments may alter firms' strategies. Another limitation is that the study primarily relies on company documents. This helps to ensure data accuracy and firm alignment, but it may reflect corporate framing or omit undisclosed internal governance processes or market pressures. Additionally, the qualitative coding in the analysis of the strategies involves interpretive judgment which can potentially contain bias even though definitions are operationalized. Finally, this study is interpretive, and case focused rather than statistical. The objective of this is to explore patterns and contingencies rather than infer causal relationships. The results demonstrate theoretical rather than generalized findings, highlighting how AI regulatory fragmentation can influence standardization versus adaptation dynamics but it does not fully predict firm behavior.

Future Research

Future research could extend this study by examining a broader set of AI intensive firms, including smaller SaaS providers and non-SaaS digital platforms, to test whether similar hybrid and localization patterns emerge. Comparative studies that incorporate additional regulatory regimes, such as the UK or key Asian jurisdictions, would help clarify how different rule configurations shape strategic responses. Longitudinal or mixed method designs could also link architectural choices more directly to performance, compliance outcomes, and customer trust, providing stronger evidence on the effectiveness of alternative adaptation strategies.

Conclusion

International SaaS firms respond to AI regulatory fragmentation by adopting varying hybrid and adaptation strategies across regions. Firms localize where regulatory risk and data sensitivity are high while maintaining a global product core to preserve economies of scale. The hybrid strategy emerges as an equilibrium that balances compliance, speed, and performance. Full adaptation strategies are reserved for firms with more infrastructure control and more regulatory pressure. Through analyzing how AI regulatory fragmentation influences strategic choices, this study contributes to the discussion of how AI regulation dynamics impact international business strategy in this uncertain and ever evolving era of AI innovation.

References

Ang, Z., & Massingham, P. (2007). National culture and the standardization versus adaptation of knowledge management. *Journal of Knowledge Management, 11*(2), 5–21.

Baker, S. R., Bloom, N., & Davis, S. J. (2016). Measuring economic policy uncertainty. *Quarterly Journal of Economics, 131*(4), 1593–1636.

Coche, E., Kolk, A., & Ocelík, 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.

de Elizalde, F. (2025). Fragmenting consumer law through data protection and digital market regulations: The DMA, the DSA, the GDPR, and EU consumer law. *Journal of Consumer Policy, 48*(3), 355–389.

Dess, G. G., & Beard, D. W. (1984). Dimensions of organizational task environments. *Administrative Science Quarterly, 29*(1), 52–73.

Duncan, R. B. (1972). Characteristics of organizational environments and perceived environmental uncertainty. *Administrative Science Quarterly, 17*(3), 313–327.

European Commission. (n.d.-a). *AI Act: Regulatory framework for AI (Application timeline).*

European Commission. (n.d.-b). *European AI Office.*

European Parliamentary Research Service. (2025). *AI Act implementation timeline (EPRS At a Glance).*

European Union. (2024). *Regulation (EU) 2024/1689 … laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).* Official Journal of the European Union (12 July 2024).

Farhad, M. A. (2024). Consumer data protection laws and their impact on business models in the tech industry. *Telecommunications Policy, 48*(9), 102836.

GDPR Local. (2025). *AI regulations in the US: What you need to know in 2025.* GDPR Local.

Ghemawat, P. (2001). Distance still matters: The hard reality of global expansion. *Harvard Business Review, 79*(8), 137–147.

Heiber, J. G., & Workman, G. (2023). The EU Data Act: A misguided policy. U.S. Chamber of Commerce.

HIPAA Journal. (2024). *When AI technology and HIPAA collide.* HIPAA Journal.

Kumar, D. (2024). Bringing Copilot to more customers worldwide—Across life and work. *Microsoft 365 Blog.*

Lawrence, P. R., & Lorsch, J. W. (1967). *Organization and environment: Managing differentiation and integration.* Harvard Business School, Division of Research.

Liu, Y., & Shi, Y. (2020). Behind the scenes: Addressing dual pressures for product standardization and adaptation in new product development in multinational corporations. *European Journal of Marketing, 54*(5), 1061–1085.

López González, J., Ferencz, J., & van der Marel, E. (2022). *Data flows: Breaking up the trade–tech puzzle (OECD Trade Policy Paper).* OECD Publishing.

Menzies, J., Sabert, B., Hassan, R., & Prince, K. M. (2024). Artificial intelligence for international business: Its use, challenges, and suggestions for future research and practice. *Thunderbird International Business Review, 66*(2), 185–200.

Microsoft Corporation. (2025a). *Annual report 2025.* Microsoft Investor Relations.

Microsoft Corporation. (2025b). *Form 10-K for fiscal year ended June 30, 2025.* U.S. Securities and Exchange Commission.

Microsoft. (2024a). *Company overview.* Microsoft Investor Relations.

Microsoft. (2024b). *EU Data Boundary documentation change log.* Microsoft Learn – Privacy.

Microsoft. (2024c). *Microsoft AI code of conduct.* Microsoft Learn.

Microsoft. (2024d). *Plan for Microsoft 365 Multi-Geo.* Microsoft Learn.

Microsoft. (2025a). *Advanced data residency in Microsoft 365.* Microsoft Learn.

Microsoft. (2025b). *Data, privacy, and security for Microsoft 365 Copilot.* Microsoft Learn.

Microsoft. (2025c). *Microsoft 365 Multi-Geo.* Microsoft Learn.

Microsoft. (2025d). *Microsoft 365 roadmap.* Microsoft.

Microsoft. (2025e). *What is the EU Data Boundary?* Microsoft Learn – Privacy.

Microsoft. (n.d.). *Microsoft 365 Copilot overview.* Microsoft Learn.

Microsoft Tech Community. (2025, September 15). Copilot Chat comes to the Microsoft 365 apps. *Microsoft Tech Community.*

Microsoft Trust Center. (n.d.). *GDPR overview.* Microsoft.

Milliken, F. J. (1987). Three types of perceived uncertainty about the environment: State, effect, and response. *Academy of Management Review, 12*(1), 133–143.

Nafizah, U. Y., Roper, S., & Mole, K. (2024). Estimating the innovation benefits of first-mover and second-mover strategies when micro-businesses adopt artificial intelligence and machine learning. *Small Business Economics, 62*(1), 411–434.

Oracle. (2024). *Oracle EU Sovereign Cloud for Fusion Applications: Datasheet.* Oracle.

Oracle. (2025a). *EU Sovereign Cloud.*

Oracle. (2025b). *FAQs: Oracle Analytics Generative AI.* Oracle Analytics Cloud Documentation.

Oracle. (2025c, August 28). *Generative AI – Release Notes (EU Sovereign Central Availability).* Oracle Cloud Infrastructure Documentation.

Oracle. (2025d, September 29). *Overview of generative AI service.* Oracle Cloud Infrastructure Documentation.

Oracle Corporation. (2025a). *Form 10-K for fiscal year ended May 31, 2025.* U.S. Securities and Exchange Commission.

Oracle Corporation. (2025b). Oracle announces fiscal 2025 fourth quarter and fiscal full year financial results. *Oracle Newsroom.*

Reuters. (2024). Salesforce closes 1,000 paid 'Agentforce' deals, looks to robot future. *Reuters.*

Ryans, J. K., Jr., Griffith, D., & White, D. S. (2003). Standardization/adaptation of international marketing strategy: Necessary conditions for the advancement of knowledge. *International Marketing Review, 20*(6), 588–603.

Salesforce. (2025a, August 5). *Artificial intelligence acceptable use policy.* Salesforce.

Salesforce. (2025b). *Data residency & resilience solutions.*

Salesforce. (2025c). *Einstein Trust Layer.* Salesforce Help.

Salesforce. (2025d). *Einstein Trust Layer: Region and language support.* Salesforce Help.

Salesforce. (2025e). *Hyperforce European Union Operating Zone.*

Salesforce Blog. (2020, September 29). Model cards for AI model transparency. *Salesforce Blog.*

Salesforce Release Notes. (2025). *Agentforce: Release and feature updates.* Salesforce Release Notes.

Salesforce, Inc. (2025a). *Form 10-K for fiscal year ended January 31, 2025.* U.S. Securities and Exchange Commission.

Salesforce, Inc. (2025b). *Salesforce announces fourth quarter and fiscal year 2025 results.* Salesforce Newsroom.

Shaw, F. X. (2024). Ignite 2024: Why nearly 70% of the Fortune 500 now use Microsoft 365 Copilot. *Official Microsoft Blog.*

TelecomTV. (2024). Oracle ups European sovereignty play with $3bn investment. *TelecomTV.*

TechRadar Pro. (2025, October). Microsoft 365 Copilot will be automatically installed… (not in the EEA). *TechRadar Pro.*

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal, 18*(7), 509–533.

Trivedi, M., & Gautam, J. K. (2025). Transforming cross-border trade with the advancement of digital platforms: An analysis. *Journal of International Economics, 16*(1), 33–44.

Vanessa, R. (2024). Artificial intelligence, digital trends and globalization: Future research trends. *FIIB Business Review, 13*(3), 286–293.

Venaik, S., & Midgley, D. F. (2019). Archetypes of marketing mix standardization–adaptation in MNC subsidiaries: Fit and equifinality as complementary explanations of performance. *European Journal of Marketing, 53*(2), 366–399.

Vogelezang, F. (2022). *The Data Act: Five implications for the datasphere*. Datasphere Initiative.

Biography

Grace is originally from Connecticut, United States. She moved to Rome in 2022 to attend John Cabot University, where she is completing a double major in International Business and Economics & Finance, with a minor in Computer Science. After earning her bachelor's degree, she plans to pursue a master's program focused on fintech and artificial intelligence. She aims to build a meaningful career in fintech, contributing to the design and development of the financial systems of the future.