Business Model Responses to Consumer Circumvention: Lessons from Piracy Applied to VPN-Enabled Geo-Arbitrage

Master thesis by Tim Weckbach
Date of submission: 17.02.2026

1. Review: William Schütte
2. Review: Prof. Dr. Alexander Kock
Darmstadt

TECHNISCHE UNIVERSITÄT DARMSTADT

Business Informatics

Technology and Innovation Management

Abstract

This thesis examines the strategic conflict between corporate price discrimination and consumer-driven geo-arbitrage using Virtual Private Networks (VPNs) in digital subscription markets. Using a mixed-methods design, the study first measures the economic motivation for digital geo-arbitrage through the Digital Services Price Index (DSPI), a price ratio index benchmarked against the US market. Analysis of up to 11 services across 11 countries reveals discounts of up to 90% in markets like Turkey and Pakistan, yet a Price-to-Wage (PTW) ratio shows an "Affordability Paradox": these services remain more expensive for local consumers relative to their income.

An Large Language Model (LLM)-based analysis of over 25,000 sentences from corporate documents and Terms of Service (ToS) then identifies coercive and adaptive Business Model Innovation (BMI) responses. The findings show that enforcement strategies are shaped more by business model architecture than by the scale of price differences. A sharp spike in technical countermeasures beginning in 2022, driven primarily by YouTube, signals an escalating arms race between platform control and technical bypass. The thesis concludes that adaptive strategies such as pricing or platform innovation may prove more sustainable than coercive enforcement, mirroring the music industry's shift from Digital Rights Management (DRM) enforcement to convenient streaming.

Keywords: Price Discrimination, Geo-Arbitrage, BMI, VPN, DSPI

Contents

1. Introduction **6**

1.1. Background and Context 6
1.2. Problem Statement 8
1.3. Research Questions (Research Questions (RQs)) 9

2. Theoretical Foundations & Literature Review **10**

2.1. Economic Foundations of International Price Setting 10
2.1.1. Third-Degree Price Discrimination 10
2.1.2. Purchasing Power Parity (Purchasing Power Parity (PPP)) as a Benchmark 11
2.2. Consumer Circumvention and the Piracy Parallel 13
2.2.1. The Piracy Analogue 13
2.2.2. The Three-Level Mechanism of Circumvention 15
2.3. Strategic Management and Business Model Innovation 16
2.3.1. Dimensions of Business Model Innovation 17
2.3.2. Theoretical Framework: Protection vs. Pricing 18
2.3.3. Platforms and Ecosystem Control 19
2.4. Research Gap 21

3. Methodology **23**

3.1. Research Design 23
3.2. Phase 1: Quantitative Data Collection (for RQ1) 24
3.2.1. Data Collection 24
3.2.2. Data Analysis 26
3.3. Phase 2: Qualitative Data Collection & Analysis (for RQ2) 27
3.3.1. Coding Procedure 27
3.3.2. Automated Text Classification 27
3.3.3. Model Selection 27
3.3.4. Operationalization of Constructs (The Coding Scheme) . . 28
3.3.5. Pipeline Architecture and Implementation 29

3.3.6. Methodological Validation: Gemini vs. Zero-Shot BERT . . 31
3.3.7. Standard Qualitative Coding 33
3.4. Data Analysis Procedures 35
3.4.1. Statistical Analysis of the DSPI 35
3.4.2. Interpretation of Qualitative Classifications 36

4. Results **37**
4.1. Dataset Overview 37
4.2. The Landscape of International Pricing: Findings from the DSPI . 37
4.2.1. Scale of the Arbitrage Incentive 38
4.2.2. Temporal Evolution of Enforcement 42
4.3. Deep Dive: Service-Specific Strategic Evolution 43
4.3.1. High-Confidence Findings: The Core Clauses 44
4.3.2. The Affordability Paradox: Real vs. Nominal Cost 45
4.4. Correlation Analysis: The Strategic Trade-off 47
4.5. Strategic Shifts and Fortress Index Ranking 51

5. Discussion **53**
5.1. Strategic Archetypes 53
5.1.1. The Content Fortress: Defensive Value Capture 55
5.1.2. The Ecosystem Fortress: Adaptive Value Proposition 56
5.1.3. The Enterprise Fortress: Identity-Based Value Capture . . 57
5.1.4. The Utility Paradox (Adobe) 58
5.1.5. The Adversarial Cycle: A View Over Time 60
5.2. The Secret Tech Race 64
5.3. Aggregate Enforcement Trends 65
5.3.1. Service-Level Enforcement Trends 66
5.4. Implications for Policy and Practice 67
5.4.1. Implications for Platform Operators 67
5.4.2. Implications for Regulators 68
5.4.3. Implications for Consumers 69
5.5. Limits of the study 70
5.5.1. Sample Size and Generalizability 70
5.5.2. The “Average Citizen” Bias (Socioeconomic Mismatch) . . 71
5.5.3. AI Classification Reliability 72

5.5.4. Document-Based Analysis Limitations 72
5.5.5. Methodological Reflections 73

6. Conclusion **74**
6.1. Summary of Key Findings 74
6.2. Contribution to Research 76
6.2.1. Methodological Contributions 76
6.2.2. Theoretical Contributions 77
6.3. The Future 78
6.3.1. Regulatory Evolution 78
6.3.2. Technological Evolution 79
6.3.3. Market Convergence 79
6.3.4. Future Research 80

A. Detailed Service Evolution **81**

B. Quantitative Reference Data **84**

Bibliography **86**

List of Figures **95**

List of Tables **97**

Glossary and Acronyms **99**

Declaration on the Use of AI-Based Tools **101**

1. Introduction

This chapter provides an overview of the research and highlights its significance. It introduces the central research problem: digital services naturally cross borders, but platforms attempt to maintain geographic pricing boundaries. By defining the problem and research questions, this chapter lays out the structure of the thesis.

1.1. Background and Context

The global digital economy has a basic contradiction: while digital services are globally accessible and deliver everywhere similar value, companies in this space commonly use, among other price discrimination strategies, geographically segmented pricing strategies (Goldfarb & Tucker, 2019). Major platforms such as Netflix, Spotify, and Microsoft 365 divide the world into different pricing regions, charging very different prices for the same digital products depending on where the customer is. This practice, known as third-degree price discrimination (Belleflamme & Peitz, 2015; Odlyzko, 2003), lets firms get the most revenue from each market by matching prices with what local users can pay. In markets with lower incomes, services are offered at much lower prices to reach more customers, while wealthier regions face higher prices. This splitting of the digital economy into regional pricing zones reflects broader tensions in digital capitalism (Srnicek, 2017).

However, the technical setup that enables global digital distribution also lets customers challenge these boundaries. The global VPN market has grown rapidly, reaching an estimated $44.6 billion in 2022 and projected to exceed $137 billion by 2030 (Grand View Research, 2023). While privacy protection remains the primary stated reason for VPN adoption, surveys consistently show that accessing geo-restricted content and obtaining better prices rank among the top motivations for consumer VPN use (Security.org, 2023). An estimated 31% of internet users worldwide have used a VPN at least once (GWI (GlobalWebIndex), 2023), with

adoption rates highest in markets with significant content restrictions or price differentials, precisely the markets where geo-arbitrage is most profitable.

Many users have discovered that VPNs can be used not only for privacy but also to bypass regional price blocks. By hiding their true location and routing their internet traffic through servers in other regions, users can change their location of subscription to access regionally restricted content libraries or purchase subscriptions at prices meant for markets with very different economic and regulatory conditions. This practice, called "digital geo-arbitrage" or "VPN price or licensing hopping" (used synonymously in this thesis), is a form of consumer driven market arbitrage that takes advantage of the price and library differences created by firms (Ariyarathna, 2022).

The economic impact of this is large. While precise figures on revenue losses from geo-arbitrage remain unavailable in the academic literature, companies treat detection rates and revenue impact assessments as commercially sensitive, the scale of the driver is clear from the pricing data itself. For individual consumers, the savings can be substantial: a user subscribing to five digital services through a low-price region could save over $100 per month compared to their home-country prices, easily justifying the $5-12 monthly cost of a commercial VPN subscription. This asymmetry between modest circumvention costs and significant potential savings creates a powerful economic incentive that purely technical barriers struggle to overcome.

This pattern parallels the digital piracy wave of the early 2000s, where users used technical tools to bypass blocks (Oberholzer-Gee & Strumpf, 2007). Just as file-sharing enabled users to bypass payment systems, VPN-enabled geo-arbitrage allows users to bypass pricing, though they still pay for the service. In both cases, consumers employ accessible technology to circumvent barriers. This forces companies to innovate on their revenue models and develop new business strategies, just as the rise of piracy ultimately led to the emergence of new streaming business models such as Spotify and Netflix (Aguiar & Waldfogel, 2018a). However, as discussed in Chapter 5, this cycle of bypassing is met by more advanced, often secret, detection technologies that try to unmask VPN users. These methods remain difficult to study, as companies treat their detection mechanisms as proprietary, making them a "black box" for researchers.

1.2. Problem Statement

The main problem this thesis looks at is the tension between firms' efforts to maintain segmented markets and consumers' ability to circumvent geographic restrictions. Subscription companies face a fundamental trade-off between two competing imperatives. On the one hand, the **economic imperative** demands that firms offer substantially lower prices in emerging markets while maintaining premium pricing in wealthier regions, in order to maximize market penetration and revenue. On the other hand, the **technical reality** is that the internet enables users to circumvent geographic restrictions using readily accessible VPN services. This conflict forces companies to rethink their strategies. They must choose between "Coercive" strategies that try to keep markets separate through technical blocking, "Adaptive" strategies that reduce the reason for arbitrage by making prices more similar, or entirely new types of business models that operate fundamentally differently.

The challenge gets worse because these two goals are not independent. Raising prices in low-income markets to reduce the arbitrage motivation undermines the economic reasoning for price discrimination in the first place, potentially losing those markets to competitors or to piracy. Conversely, investing in ever more sophisticated blocking technologies generates recurring costs, creates friction for legitimate travelers, and risks alienating the very users firms seek to keep. This creates what can be described as a discrimination dilemma: the more aggressively a firm discriminates on price, the greater the arbitrage incentive and the higher the enforcement costs required to maintain market segmentation (Tirole, 1988). The dilemma is further complicated by the asymmetric nature of the contest: while firms must invest in detection systems that work across all users, circumvention tools need only succeed for some users some of the time to remain commercially viable.

1.3. Research Questions (RQs)

To analyze this conflict, this thesis addresses two main research questions that address both why users engage in geo-arbitrage and how companies respond to it.

The first research question focuses on measuring the economic driver: **RQ1 (The Economic Incentive):** *To what extent does international price differentiation for digital services deviate from local purchasing power (based on local wages), and what degree of economic incentive does this create for consumer-driven geo-arbitrage?*

To answer this, we built the DSPI, which compares nominal subscription prices across regions relative to a US baseline. We complemented the DSPI with a separate PTW ratio that measures how affordable these subscriptions are relative to local wages. The difference between nominal price (the sticker price in USD) and real affordability (the cost relative to local income) is key: a service may seem cheap to a foreign user while being expensive for a local.

The second research question examines how companies respond to the arbitrage threat: **RQ2 (The Strategic Response):** *How do digital service providers strategically frame the issue of circumvention, and to what extent can a shift towards coercive or adaptive business model responses be measured in their corporate disclosures over time?*

To answer this, we used AI to analyze and classify ToS documents and annual reports, grouping company language into categories like “Technical Blocking,” “Legal Threat,” and “Price Discrimination.” Looking at data over time lets us see how strategies have changed from 2020 to 2025.

2. Theoretical Foundations & Literature Review

This chapter builds the theoretical framework by looking at three areas: economic pricing, consumer behavior, and business model innovation. By connecting Hal Varian's work on price discrimination with the history of digital piracy, we create a way to understand modern geo-arbitrage as a major challenge for digital companies.

2.1. Economic Foundations of International Price Setting

To understand why consumers engage in geo-arbitrage, we first need to understand why firms create the price gaps that make such arbitrage worthwhile. Geographic price differences are not random, they follow well-known economic principles.

2.1.1. Third-Degree Price Discrimination

According to Varian (1989), third-degree price discrimination happens when a firm divides the market based on visible traits—in this case, geographic location—and charges different prices to each group. For digital goods, where the cost of copying is near zero ($MC \approx 0$) (Amit & Zott, 2001; Shapiro & Varian, 1998), this strategy allows firms to get the most consumer surplus from both high-income (e.g., Switzerland) and low-income (e.g., Turkey) markets at the same time.

Two conditions must hold for successful price discrimination. First, *market segmentation* requires that the firm be able to distinguish between consumer groups based on observable characteristics (such as IP address or billing location). Second, the *no-arbitrage condition* requires that the firm be able to prevent the resale or

transfer of the good between segments, a condition rooted in the economics of intellectual property rights (Stiglitz, 2008). VPN-enabled geo-arbitrage directly breaks *Condition 1*, effectively merging the different regions into a single global market. Duch-Brown and Martens (2016) demonstrate that geo-blocking has become the primary mechanism for maintaining this segmentation in digital content markets.

This study also suggests that companies accidentally segment their customers into sub-groups within high-income regions. By maintaining detection mechanisms (such as VPN blocking), companies effectively segment the market based on user willingness to exert effort. This creates a division between "active" users—those who spend time and effort to bypass blocks, and "passive" users who prefer convenience. In this way, technical friction functions as a self-selection mechanism (Shapiro & Varian, 1998): companies retain high revenue from the majority of users while tolerating marginal losses from a small group of technically proficient users.

2.1.2. Purchasing Power Parity (PPP) as a Benchmark

The "Law of One Price" suggests that in an efficient market, identical goods should sell at the same price when shown in a common currency (Pakko & Pollard, 2003). However, differences from this law are common. Indeed, Engel and Rogers (2004) demonstrate that price convergence remains incomplete even under economic integration, as firms actively maintain price differentials through market segmentation. Rogoff (1996) argues that for physical goods, shipping costs and trade barriers justify price differences. In the digital world, Clemons et al. (2002) note that while transaction costs are much lower, price differences continue because firms can set up detailed customer segmentation. Blum and Goldfarb (2006) provide important evidence that digital goods do not fully "defy the law of gravity": even in online commerce, geographic distance and national borders and regulations continue to affect trade patterns, suggesting that physical-world frictions partially persist in digital markets. The Billion Prices Project (Cavallo & Rigobon, 2016) has further demonstrated that online price data can

serve as a reliable tool for measuring cross-country price differences, providing methodological precedent for the DSPI developed in this thesis.

The concept of PPP has a long history in economics, originating from Gustav Cassel's work in the early twentieth century (Cassel, 1918) and later formalized through the Balassa-Samuelson hypothesis, which predicts that price levels tend to be higher in countries with higher productivity (Balassa, 1964). In its absolute form, PPP posits that a basket of goods should cost the same everywhere after currency conversion. In its relative form, it predicts that exchange rate changes should offset inflation differentials over time. For digital goods, however, neither form fully applies: there are no shipping costs, no tariffs, and no physical constraints on distribution. The marginal cost of serving an additional user in any country is effectively zero. This means that price differences for digital services are almost entirely a function of deliberate corporate strategy rather than cost-driven economic forces (Goldfarb & Tucker, 2019; Shapiro & Varian, 1998).

We use PPP as a benchmark for "economically justified" pricing. If a Netflix subscription in Turkey is cheaper than in the US only because of currency value and local purchasing power, this fits standard economic theory. However, if the price difference is bigger than what PPP adjustments would predict, it creates a "above-normal" arbitrage motivation, a price gap that motivates bypassing beyond simple purchasing power factors. We measure this through the DSPI.

It is important to distinguish between two types of price dispersion (Varian, 1989). First, "welfare-enhancing" price discrimination occurs when firms lower prices in poorer markets to expand access, effectively subsidizing digital inclusion. Second, "rent-extracting" price discrimination occurs when firms charge higher prices in wealthy markets not because costs are higher, but because consumers' willingness to pay is greater (Odlyzko, 2003; Stiglitz, 2008). The combination of both creates the asymmetric incentive structure at the heart of geo-arbitrage: the welfare-enhancing discount in one market becomes the rent-extraction loophole exploited by consumers from another.

2.2. Consumer Circumvention and the Piracy Parallel

Consumer-driven arbitrage is not new (Anson et al., 2019). The digital "geo-arbitrage" pattern can be understood through the history of digital piracy.

2.2.1. The Piracy Analogue

Oberholzer-Gee and Strumpf (2007) showed that file-sharing forced the music and film industry to change its business model, eventually leading to legitimate digital distribution platforms like iTunes, Spotify and Netflix. Subsequent research confirmed that while piracy displaced some sales, it also drove innovation toward legitimate distribution platforms (Waldfogel, 2010). This historical precedent provides a framework for understanding VPN-based geo-arbitrage. Similarly, geo-arbitrage works as a market signal, showing a basic mismatch between rigid regional pricing structures and the borderless reality of the global internet. This division has been described as a "Splinternet" (Masnick, 2019), where the same service exists in different versions across different regions.

The parallel is useful: just as Napster and BitTorrent exposed the music industry's failure to meet consumer demand for convenient digital access, VPN-enabled price hopping highlighted the sustainability challenges of global price discrimination. In both cases, users innovated before companies adapted. The sudden shutdown of Megaupload in 2012 demonstrated both the scale of piracy and the limits of enforcement-only approaches (Danaher & Smith, 2014). France's "graduated response" law (HADOPI) provided further evidence: while Danaher et al. (2014) found a modest positive effect on iTunes sales, the law did not eliminate piracy but rather displaced it to harder-to-track channels. Similarly, Reimers (2016) found that copyright protection measures have measurable effects on legitimate sales, confirming that piracy and legitimate consumption are connected rather than independent phenomena.

The transition from piracy to legitimate consumption was not automatic. It required significant business model innovation. Aguiar and Waldfogel (2018a) found that the growth of music streaming displaced both piracy and legitimate purchases,

suggesting that convenient, affordable access can serve as a substitute for unauthorized consumption. This finding is directly relevant to geo-arbitrage: if the price gap between regions were smaller, or if services offered globally uniform access, the motivation for VPN-based circumvention would diminish, just as affordable streaming reduced the motivation for file-sharing.

As we discuss later (Chapter 5), companies are likely improving their ability to accurately geolocate users. However, empirical verification remains difficult because the technical details are proprietary, similar to the piracy case of DRM protection.

The broader literature on digital piracy confirms that enforcement alone rarely eliminates unauthorized access (Peukert et al., 2017). Déjean (2009) argue that piracy can even function as a "sampling mechanism," where unauthorized access leads to subsequent legitimate purchases, a dynamic that may also apply to geo-arbitrage, where users who discover a service at a lower price may later convert to full-price subscribers when enforcement tightens. However, key differences emerge between piracy and geo-arbitrage. In terms of *access versus price*, piracy was often about getting content that was not available at all, while geo-arbitrage concerns obtaining a more favorable price; piracy involved no payment, whereas geo-arbitrage involves payment at a reduced rate. Regarding *legal status*, piracy is clearly illegal, while geo-arbitrage occupies a gray zone (Ariyarathna, 2022), as users pay for real accounts but misrepresent their geographic location. Finally, in terms of *industry response*, the music industry eventually adapted with streaming services, and whether companies will adopt similar adaptive responses to geo-arbitrage is a central question of this thesis.

A closely related form of circumvention that bridges piracy and geo-arbitrage is *password sharing*, where subscribers share their account credentials with non-paying users. Chen and Sheng (2026) model the economics of password sharing in digital subscription markets, demonstrating that it creates a structurally similar tension between platforms' revenue protection and consumer surplus maximization. Like geo-arbitrage, password sharing involves a genuine subscriber account (unlike piracy), but undermines the platform's value capture by extending access beyond the intended paying user base. Netflix's high-profile crackdown on password sharing beginning in 2023, which coincides precisely with the broader

enforcement surge documented in our ToS analysis (Table 9), illustrates how platforms increasingly treat all forms of access circumvention, whether geographic or credential-based, as strategic threats requiring coordinated enforcement responses. This suggests that geo-arbitrage should not be studied in isolation but as part of a broader spectrum of consumer-driven circumvention behaviors that collectively challenge digital subscription business models.

2.2.2. The Three-Level Mechanism of Circumvention

Drawing from the self-control framework applied by Higgins et al. (2008) to digital piracy, we propose that the decision to engage in geo-arbitrage can be modeled as a three-level mechanism. This way of looking at it helps explain why otherwise law-abiding consumers engage in "digital smuggling":

Individual Level: Rational Choice and Personal Risk

At the individual level, the consumer performs a cost-benefit analysis. The financial gain (e.g., an 83% discount on YouTube Premium from Turkey) is weighed against the perceived probability of detection and the severity of punishment (Ransbotham & Mitra, 2009) (e.g., account termination). When enforcement is perceived as inconsistent, the perceived risk may be low. Crucially, the expected utility calculation is heavily skewed in favor of circumvention: even if one assumes a moderate probability of detection (say, 20% to 30%), the worst-case outcome (account termination with refund of remaining subscription) is far less severe than the punishment for comparable physical-world arbitrage (e.g., customs seizures, import duties, legal penalties). This asymmetry between potential gain and potential loss creates a rational incentive for risk-neutral consumers to attempt geo-arbitrage, consistent with expected utility theory (Becker, 1968).

Inter-personal Level: Social Influence

The behavior may be reinforced by online communities (e.g., Reddit, Discord, specialized forums). Observing others successfully using VPNs can lower the

psychological barrier to entry, consistent with social influence research (Kastanakis & Balabanis, 2012). The role of "how-to" guides and community knowledge-sharing is particularly significant: detailed tutorials with step-by-step instructions for subscribing to services through foreign accounts effectively reduce the technical skill required to near zero, democratizing what was once a practice limited to technically sophisticated users. This "knowledge diffusion" effect (Wasko & Faraj, 2005) means that as communities grow, the effective barrier to entry falls, creating a positive feedback loop between adoption and accessibility.

Societal Level: Moral Intensity

The perception of the act is key. Unlike shoplifting a physical good or pirating digital content outright, digital arbitrage may be framed by users not as theft, but as a response to pricing perceived as unfair. This framing aligns with neutralization theory (Thongmak, 2017), and reflects broader concerns about perceived price fairness in digital markets (Poort & Zuiderveen Borgesius, 2019; Xia et al., 2004). Users employ several "neutralization techniques" to justify their behavior (Sykes & Matza, 1957): (1) denial of injury ("The company still gets paid, just less"), (2) denial of victim ("These are billion-dollar corporations"), (3) condemnation of the condemner ("They charge unfair prices"), and (4) appeal to higher loyalties ("I'm supporting the service by subscribing instead of pirating"). The moral ambiguity is heightened by the fact that geo-arbitrage, unlike piracy, involves a genuine financial transaction, where the user pays for the service, just at a price not intended for their market.

2.3. Strategic Management and Business Model Innovation

Faced with this disruption, firms must adapt. We analyze their responses using BMI. As defined by Wirtz et al. (2016), theorized by Teece (2010), and grouped by Foss and Saebi (2017), BMI means rethinking the value offer and delivery methods in response to outside shocks.

2.3.1. Dimensions of Business Model Innovation

To carefully analyze how firms adapt, we divide their business models into three parts, following the widely used three-part framework (Amit & Zott, 2012; Teece, 2010):

The first dimension is the **Value Proposition** (what is offered): the core product or service and the bundle of benefits it provides to the customer. In digital streaming, this is the content library and the convenience of "watch anywhere" access. As Osterwalder and Pigneur (2010) emphasize, the value proposition is the fundamental reason why customers choose one provider over another, and it must be continuously adapted to changing market conditions.

The second dimension is **Value Delivery** (how it is reached): the channels and technical infrastructure used to deliver the value. This includes the streaming platform, the Content Delivery Network (CDN) (where latency and infrastructure variability play a significant role), and the user interface. Crucially, it also includes the *geographic segmentation* logic that determines who can access what. The delivery mechanism is particularly relevant because digital services, unlike physical goods, are consumed at the point of delivery, making the delivery infrastructure itself a point of control (Goldfarb & Tucker, 2019).

The third dimension is **Value Capture** (how money is made): the revenue model and the mechanisms to sustain profitability (Amit & Zott, 2012). This includes the pricing strategy (e.g., price discrimination) and the enforcement mechanisms used to prevent revenue leakage (e.g., blocking arbitrage). Zott et al. (2011) note that value capture is often the most contested dimension in platform-based business models, as multiple stakeholders compete over the distribution of value.

VPN-enabled arbitrage fundamentally attacks the **Value Capture** dimension by breaking the link between location and price. It also exploits the **Value Delivery** infrastructure (the open internet). However, the impact on the **Value Proposition** is indirect but significant: if enough users circumvent regional restrictions, firms may be forced to reevaluate what they offer in each market (e.g., by shifting to globally available original content rather than regionally licensed catalogs).

Based on this, we expect firm responses to fall into two types of innovation. This dual-response framework aligns with research on strategic agility, which shows that firms capable of both defensive and adaptive innovation outperform those relying on a single approach (Karimi & Walter, 2020). The first is **coercive innovation** (Value Capture focus), which reinforces the barriers to protect the existing model through technical blocking and legal threats. The second is **adaptive innovation** (Value Proposition focus), which changes the product offer to make arbitrage irrelevant, for example through global pricing or ecosystem lock-in.

2.3.2. Theoretical Framework: Protection vs. Pricing

Digital strategy and arbitrage have been widely discussed. Johnson et al. (2008) define the necessity of business model reinvention when facing disruptive shifts, while Granados et al. (2006) show how e-commerce increases market efficiency by making arbitrage easier. However, Anson et al. (2019) note that cross-border arbitrage responds to exchange rate differentials in ways that create strategic challenges for firms, leading to complex responses such as those described by Thongmak (2017) in the context of digital piracy. Beunza and Stark (2004) also argue that price is ultimately a social construct, heavily influenced by the "material sociology" of the market—in this case, the VPN technology that alters the visibility of the consumer.

To categorize firm responses, we adopt the framework established by Sundararajan (2004) on managing digital piracy, mapping it to our BMI dimensions. The first category is **protection** (coercive / Value Capture), which increases the technological or legal costs of circumvention, attempting to *repair* the broken Value Capture mechanism. The second is **pricing** (adaptive / Value Proposition), which adjusts the business model through pricing and versioning to lower the economic motivation for arbitrage, effectively *innovating* the Value Proposition to be less sensitive to location. Firms face a fundamental trade-off: Is the cost of enforcing market segmentation (repairing Value Capture through blocking technology and legal resources) lower than the revenue lost to arbitrage?

This trade-off can be formalized through the lens of game theory (Tirole, 1988). The interaction between a platform and its users constitutes a sequential game:

the firm chooses an enforcement level e (at cost $C(e)$), and users observe this enforcement level and decide whether to attempt arbitrage based on their perceived probability of detection $p(e)$. The firm's optimization problem is to choose e^* that maximizes profit:

$$\max_e \left[R_{\text{legitimate}}(e) - R_{\text{lost}}(e) - C(e)\right] \tag{2.1}$$

where $R_{\text{legitimate}}$ is revenue from customers paying full price, R_{lost} is revenue lost to successful arbitrage, and $C(e)$ is the cost of enforcement. The key insight is that $C(e)$ is convex (each marginal unit of enforcement is more expensive than the last), while $R_{\text{lost}}(e)$ is concave (diminishing returns from blocking additional arbitrageurs). This implies an interior optimum: perfect enforcement is never optimal, and some level of "tolerated arbitrage" is economically rational (Becker, 1968). This theoretical prediction aligns with our empirical finding that no firm in our sample achieves (or apparently attempts) 100% blocking effectiveness.

The game-theoretic framing also explains why different firms choose such different enforcement levels. A firm's optimal e^* depends on: (1) the price gap across markets (larger gaps increase R_{lost} and shift e^* upward), (2) the marginal cost of enforcement technology (streaming services face lower marginal costs for IP-blocking than software firms do for license verification), and (3) the elasticity of user circumvention behavior to enforcement intensity (if users quickly adapt to new blocking measures, the effective $p(e)$ declines over time, reducing the return on enforcement investment).

2.3.3. Platforms and Ecosystem Control

Digital platforms operate within a fundamental tension between growth and control. To attract users and content creators, platforms must maintain a degree of openness that facilitates participation and innovation. However, to protect revenue streams and maintain quality, platforms must also exercise control over who accesses what content and at what price point. This tension is central to

platform economics, as described by Rochet and Tirole (2003), who model two-sided markets where platforms must balance the interests of multiple user groups simultaneously.

VPN providers exploit this tension. They use the platform's content (e.g., Netflix's streaming library) while bypassing its payment rules (regional pricing). This creates a technical and strategic cycle of countermeasures and counter-countermeasures. **Coercive strategies** include legal threats embedded in ToS, IP address blocking, payment verification requirements, and strict geographic checks on billing addresses; these aim to restore the segmentation condition required for price discrimination, but they impose costs on both the platform (technology investment, user friction) and legitimate users (false positives, reduced portability). **Adaptive strategies**, by contrast, involve standardizing global prices to eliminate the arbitrage motivation, creating ecosystem lock-in through hardware integration (e.g., Apple's approach), or developing content exclusive to specific regions rather than restricting access to a global catalog. These strategies accept some loss of price discrimination power in exchange for reduced enforcement costs and improved user experience.

The broader trend toward sharing and platform-based economies (Srnicek, 2017) further complicates geographic price boundaries, as users increasingly expect borderless access to digital services. This expectation is reinforced by the "born global" nature of digital platforms (Brouthers et al., 2016), which initially attract users with the promise of universal access before later imposing geographic restrictions as licensing and pricing complexities emerge.

Critically, Parker and Van Alstyne (2018) demonstrate that platforms face an inherent tension between openness (which drives innovation and user growth) and control (which protects revenue and quality). Their framework suggests that the optimal balance point shifts depending on platform maturity and competitive dynamics. VPN arbitrage directly exploits this fundamental trade-off, forcing platforms to reevaluate where that balance lies. The concept of "platform envelopment" (Eisenmann et al., 2011) is also relevant here: as platforms like Amazon and Apple expand into multiple service categories (shopping, streaming, cloud storage), they create ecosystem dependencies that make VPN-based arbitrage increasingly impractical, as users would need to relocate their entire digital identity,

not just a single subscription.

The strategic implications are significant: platforms that choose aggressive blocking may sacrifice user experience and brand perception, while those that tolerate arbitrage may face revenue leakage. Neither approach is without cost, and the optimal strategy likely depends on the specific business model and competitive context of each platform. As Cusumano et al. (2019) argue, the most successful platforms are those that find ways to create value for all participants while maintaining enough control to sustain their revenue models, a balance that geo-arbitrage directly threatens.

2.4. Research Gap

While price discrimination theory (Varian, 1989) and platform strategy (Parker & Van Alstyne, 2018) have been extensively researched independently, there is still a clear gap where they overlap. Although several research agendas have been proposed for BMI (Foss & Saebi, 2017), there is a lack of empirical work connecting the *size* of pricing drivers (as measured by indices like the DSPI) with the *specific strategic responses* of firms.

The existing research has three main gaps.

The first is **theoretical isolation**. Most studies focus either exclusively on the economics of pricing (e.g., optimal price discrimination strategies as modeled by Varian (1989) and Tirole (1988)) or on the legal aspects of copyright enforcement and digital rights management (Lindsay & Ricketson, 2006), but rarely examine the strategic interaction between these domains as mediated by consumer-side technology such as VPNs. Goldfarb and Tucker (2019) identify this disciplinary divide as a broader challenge in digital economics, noting that the field lacks integrative frameworks capable of connecting pricing decisions, consumer behavior, and technological countermeasures. The platform economics literature (Parker & Van Alstyne, 2018; Rochet & Tirole, 2003) has examined pricing in two-sided markets, but has not addressed the specific challenge of geographic arbitrage enabled by circumvention technology.

The second gap is a **lack of quantification**. While anecdotal evidence of geo-arbitrage is abundant in consumer forums and technology journalism, systematic quantification of the arbitrage driver across services and regions is lacking. Existing price comparison indices (such as the Big Mac Index (Pakko & Pollard, 2003) or the Billion Prices Project (Cavallo & Rigobon, 2016)) have focused on physical goods or aggregate online price levels, without developing specialized metrics for digital subscription services. The DSPI developed in this thesis addresses this gap by providing a standardized nominal price index, complemented by a separate PTW ratio that captures real affordability, together enabling cross-service and cross-country comparisons that have not been available in prior research.

The third gap is **limited strategic analysis**. Previous research on digital piracy has examined how firms respond to unauthorized copying (Danaher et al., 2014; Oberholzer-Gee & Strumpf, 2007; Peukert et al., 2017), but the distinct characteristics of geo-arbitrage (payment rather than piracy, location rather than access) warrant specialized investigation. The piracy literature has established that firms respond through a combination of legal, technical, and market-based strategies (Sundararajan, 2004), but it remains unclear how these response categories map onto the geo-arbitrage context, where the "infringing" behavior involves a genuine commercial transaction rather than theft. The coercive-adaptive split proposed in this thesis provides a framework for categorizing these responses that is specifically designed for the geo-arbitrage phenomenon.

This thesis addresses all three gaps through a mixed-methods design that combines quantitative price measurement (DSPI) with qualitative analysis of corporate enforcement documents, bridging the economic and strategic dimensions that prior work has treated in isolation.

3. Methodology

This chapter describes the research design, how data was collected, and the analysis methods used to investigate both the economic rationale for geo-arbitrage (RQ1) and the strategic responses of digital service providers (RQ2). The methods were chosen based on both research questions: quantifying price gaps requires standardized measurement, while understanding corporate strategy requires interpretive analysis of textual documents. The chapter starts with the research design, goes through both research phases, and ends with how we combined both data sets.

3.1. Research Design

This study used a sequential explanatory mixed-methods design (Creswell & Plano Clark, 2017), combining quantitative price analysis with qualitative text classification. The reason for this dual approach was to first show the *size* of the economic problem (the arbitrage driver) and then look at the *strategic responses* of the actors involved. The sequential design was appropriate because the quantitative findings (price disparities) provided necessary context for interpreting the qualitative findings (enforcement strategies): understanding *how much* firms discriminate on price was essential before analyzing *how* they protect those price differences.

The quantitative phase (Phase 1) built the “Digital Services Price Index” (DSPI) to objectively measure nominal price differences in global digital service pricing, complemented by a PTW ratio to assess real affordability relative to local wages. This phase established the dependent variable (the arbitrage driver) by collecting and normalizing subscription prices across 11 countries.

The qualitative phase (Phase 2) used a Large Language Model (LLM) pipeline to classify corporate disclosures and ToS, finding the strategic frameworks firms used

to manage or fight this variance. This phase identified the independent variable (the enforcement strategy) by systematically coding over 25,000 sentences from corporate documents into theoretically grounded categories.

The integration of both phases occurs in the Discussion (Chapter 5), where pricing patterns are mapped against enforcement intensity to identify strategic archetypes. This integration provides a full understanding of the geo-arbitrage ecosystem based on public documentation, though proprietary information and undisclosed technologies remain hidden. Specifically, firms' internal detection algorithms, real-time blocking rates, and revenue impact assessments are not accessible through public documents and represent an inherent limitation of document-based analysis.

3.2. Phase 1: Quantitative Data Collection (for RQ1)

3.2.1. Data Collection

To construct the DSPI, a representative basket of 11 digital services was selected: Netflix, YouTube Premium, Disney+, Amazon Prime, Spotify, Apple Music, Microsoft 365, Adobe Creative Cloud, Xbox Game Pass, NordVPN, and ExpressVPN. These cover Video on Demand, Music Streaming, Software/Gaming, and VPN services. Note that for the qualitative analysis (Phase 2), Xbox Game Pass data is combined with Microsoft 365 under the "Microsoft" category, as both are governed by the same Microsoft Services Agreement.

Price data was collected from a sample of 11 countries to capture the full spectrum of purchasing power. The countries included are: Argentina, Brazil, Germany, Pakistan, Philippines, Poland, Switzerland, Turkey, Ukraine, United Kingdom, and the United States. Only countries with high-confidence official wage data were included.

The country selection followed a purposive layered sampling strategy designed to maximize variance along three dimensions. First, **income level**: the sample spans from high-income OECD economies (Switzerland, USA, UK, Germany) through upper-middle-income economies (Poland, Argentina, Brazil, Turkey) to

lower-middle-income economies (Philippines, Pakistan, Ukraine), ensuring representation across the World Bank's income classifications. Second, **geographic diversity**: the sample covers Western Europe, Eastern Europe, the Americas, South Asia, and Southeast Asia, reducing the risk of region-specific confounds. Third, **arbitrage relevance**: several countries (Turkey, Argentina, Pakistan) were specifically included because they are frequently cited in consumer forums and technology journalism as popular "target" countries for VPN-based price hopping, making them directly relevant to the research questions. Countries with hyperinflationary conditions (Argentina, Turkey) were deliberately retained despite their price volatility, as they represent extreme cases that show the boundaries of price discrimination strategies.

The service selection similarly followed a purposive approach. The 11 services were chosen to represent four distinct business model categories: Video on Demand (Netflix, YouTube Premium, Disney+, Amazon Prime), Music Streaming (Spotify, Apple Music), Software/Gaming (Microsoft 365, Adobe Creative Cloud, Xbox Game Pass), and VPN Services (NordVPN, ExpressVPN). This categorization ensured that the analysis can compare enforcement strategies across fundamentally different value delivery mechanisms (streaming vs. download vs. ecosystem-embedded). The VPN providers were included as a contrasting case: as enablers of arbitrage rather than targets of it, their strategic framing provides a useful counterpoint to the defensive approaches of content and software providers. All selected services met three inclusion criteria: (1) global availability in at least 9 of the 11 sample countries, (2) a publicly accessible individual subscription tier, and (3) publicly available ToS documents spanning at least three years of the study period (2020–2025).

Data was collected using a **Digital Audit** approach, adapting the methodology established by Hannak et al. (2014) for detecting online price discrimination. A virtual presence was established in each target country using a commercial VPN service to simulate local access, a technique now standard in information systems research for "mystery shopping" in digital markets. For each service and country, the monthly "Standard" subscription price was recorded in local currency. This approach mirrors the methodology of the "Billion Prices Project" (Cavallo, 2017), which demonstrated the validity of using high-frequency online scraping

to construct robust price indices that track real-time economic disparities more effectively than traditional CPI baskets.

3.2.2. Data Analysis

The raw price data was processed in two stages, yielding two distinct metrics.

Stage 1: The DSPI (Nominal Price Index). All local prices were converted to a common currency (USD) using market exchange rates (recorded in December 2025). The DSPI was then calculated as the ratio of the local price to the US baseline price. A DSPI of 1.0 indicates price parity with the US market, while a DSPI < 1.0 indicates a cheaper market (a potential arbitrage source), and a DSPI $>$ 1.0 indicates a more expensive market. Statistical variance analysis was performed to identify which service categories showed the highest degree of nominal price discrimination.

Stage 2: The PTW Ratio (Real Affordability). As a separate complementary metric, each USD-converted price was also calculated as a percentage of the *Median National Monthly Wage* (sourced from OECD (OECD, 2023), national statistical institutes (INDEC, 2023), and economic databases (Turkish Statistical Institute, 2023); the complete list of wage figures, exchange rates, and sources is documented in Table 10 in Appendix B), giving a direct measure of the economic burden on the local consumer. This PTW ratio was proposed as a new alternative to standard PPP adjustment, arguing it better reflects subscription goods' affordability relative to disposable income in the specific context of digital services.

Note that a DSPI of 1.0 (Nominal Parity) does not imply equal affordability. Due to vast differences in median wages (e.g., Switzerland vs. Pakistan), a service priced identically in USD would be significantly more expensive for the Pakistani consumer in real terms (requiring a larger percentage of their income). Thus, the arbitrage motivation persists even at nominal parity if the local price is structured to be affordable for the local median earner. This distinction between nominal price (captured by the DSPI) and real affordability (captured by the PTW ratio) is central to understanding the full impact of digital pricing that standard economic data might miss (Brynjolfsson et al., 2019).

3.3. Phase 2: Qualitative Data Collection & Analysis (for RQ2)

3.3.1. Coding Procedure

The analysis followed a systematic coding approach inspired by the **Gioia Methodology** (Gioia et al., 2013), which organizes qualitative data into layers: 1st-order concepts (raw terms found in text), 2nd-order themes (theoretical categories such as "Technical Blocking"), and aggregate dimensions (Strategic Responses). While first designed for manual coding (Duriau et al., 2007), this layered structure provided the conceptual framework for the automated classification pipeline described below.

3.3.2. Automated Text Classification

To address the limits of traditional Natural Language Inference (NLI) models in capturing the complex legal and technical language of ToS, this study used an advanced classification pipeline with modern LLMs. Specifically, the pipeline was upgraded from a BERT-based architecture (DeBERTa-v3-large) to the *Gemini 3 Flash* model, accessed via the Google Generative AI API.

3.3.3. Model Selection

The choice of *Gemini 3 Flash* was driven by the need for deeper reasoning abilities and better context awareness. Unlike NLI models, which classify based on entailment probabilities between premises and hypotheses, generative LLMs can interpret complex sentence structures and tell the difference between ambiguous legal standard terms ("General Terms") and specific geo-arbitrage restrictions. Recent work has confirmed the viability of LLMs for automated legal analysis tasks (Carneiro-Diaz et al., 2025).

Key advantages observed during the model transition were threefold. First, the model demonstrated strong **contextual understanding**, distinguishing between benign references to "account suspension" (e.g., for fraud) and strategic "Legal Threats" tailored to prevent cross-border usage. Second, its **zero-shot performance** was notable: the model achieved high accuracy without extensive fine-tuning, utilizing a robust system prompt to align with the theoretical categories defined in Chapter 2. Third, the "Flash" architecture provided high **efficiency** and throughput, enabling the processing of the entire dataset (approx. 25,000 sentences) within a reasonable timeframe of only a few days when done in batching.

3.3.4. Operationalization of Constructs (The Coding Scheme)

Based on the theoretical framework, the following coding scheme was enforced via the LLM system prompt. This scheme maps the abstract concept of "Strategic Response" into measurable data points.

Strategic Frames

The model was tasked to identify the underlying justification provided by the firm:

Frame: Legal Compliance Justifying geo-blocking as a non-negotiable legal or contractual necessity (e.g., "Due to licensing agreements...").

Frame: Security Risks (Service Provider Frame) Arguments that VPNs/Proxies are unsafe, malicious, or compromise user data.

Frame: Privacy/Security (VPN Provider Frame) Arguments focusing on encryption, anonymity, and protection from surveillance.

Firm Actions

The model categorized specific enforcement clauses into:

Action: Technical Blocking Active technological measures to detect or block the specific use of VPNs/Proxies (e.g., “We use geo-blocking technology”, “to provide digital rights management”).

Action: Legal Threat Explicit threats of account termination, suspension, or legal action specifically for using circumvention tools.

Action: Account Action General punitive measures against accounts (termination, suspension) for broad violations. Note: in the implemented classification prompt, this category was merged into “Legal Threat” for cases specifically tied to circumvention tools and under “General Terms” for standard account-related boilerplate, resulting in zero standalone classifications (see Table 2).

Action: Price Discrimination Explicit differences in pricing based on region, currency, or purchasing power.

Action: Legitimate Portability Rules allowing temporary access while traveling (e.g., European Union (EU) Portability Regulation).

Action: General Terms Standard legal boilerplate and general contractual language (e.g., liability clauses, warranty disclaimers, general user obligations) that does not fall into any specific enforcement category. While constituting approximately 94% of the dataset, General Terms are retained in the master dataset to preserve the full document structure but are excluded from strategic trend analyses to isolate distinct enforcement categories.

3.3.5. Pipeline Architecture and Implementation

The reclassification process was automated using customized Python scripts.

System Prompt Engineering

To ensure consistent and theoretically grounded outputs, the system prompt was engineered with strict constraints. The exact prompt structure is provided below:

```
SYSTEM_PROMPT = """You are a scientific classifier.
CATEGORIES:
1. Technical Blocking: Measures/Technologies used to detect
   or block the specific use of VPNs/Proxies.
2. Legal Threat: Explicit threats of account termination,
   suspension, or legal action for using circumvention
   tools.
3. Price Discrimination: Differences in pricing based on
   region, currency, or purchasing power.
4. Content Licensing: Geographic restriction of content
   availability (e.g. 'not available in your region')
   due to rights.
5. Legitimate Portability: Rules allowing temporary access
   while traveling (e.g. EU Portability Regulation).
6. Regulatory Compliance: References to local laws, tax/VAT
   compliance, or export controls.
7. User Workaround: Descriptions of users bypassing
   restrictions (using VPNs, changing store region).
8. Security Risk: (Service Provider Frame) Arguments that
   VPNs/Proxies are unsafe, malicious, or compromise
   user data.
9. Privacy/Security: (VPN Provider Frame) Arguments
   focusing on encryption, anonymity, and protection
   from surveillance.
10. General Terms: Standard legal text, general marketing,
    or unrelated content.

INSTRUCTIONS:
- Return a JSON array of objects for the sentences in
  EXACT order.
- Format: [{"category": "Category Name",
  "confidence": 0.9}, ...]
"""
```

Listing 3.1: System Prompt used for Gemini 3 Flash Classification

Batch Processing and Error Handling

To optimize for the API's rate limits and ensure data integrity, the pipeline utilized a batch processing approach. Sentences were grouped into batches of 25 and processed in a single API call. This method significantly reduced network overhead and total processing time. A robust error-handling mechanism was implemented to manage API timeouts or rate limits (HTTP 429). The script included a "circuit breaker" to halt execution upon repeated failures and a resume function to continue processing from the last saved state.

Forward-Fill Strategy for Longitudinal Consistency

A key challenge in analyzing longitudinal ToS data is the rarity of document updates, as companies do not release new ToS documents every year. To address this, a "forward-fill" strategy was applied: whenever no new document was published for a given year, the most recent version was carried forward on the assumption that its clauses remain legally in effect until explicitly replaced. For example, if a document was released in 2020 and the next update appeared in 2023, the 2020 version was treated as active for 2021 and 2022. This ensured the dataset accurately reflected the *active* regulatory environment in every year, distinguishing between genuinely "missing data" and "persistent rules."

3.3.6. Methodological Validation: Gemini vs. Zero-Shot BERT

To validate the choice of the Gemini 3 Flash model, a comparison was done against a traditional Zero-Shot classification approach using a BERT-based model. The results showed a substantial difference between the two models, confirming the need for a modern LLM with large context windows for this specific task, consistent with recent findings on LLM performance in text annotation (Gilardi et al., 2023; Hakimi Parizi et al., 2023).

Agreement Analysis

The comparison revealed a very low agreement rate of **26.8% (Accuracy)** between the two models. Cohen's Kappa score was **0.032**, suggesting agreement effectively equivalent to random chance. This discrepancy indicated a fundamental difference in how each model interpreted the classification tasks.

The Core Conflict: Sensitivity vs. Context

The analysis highlighted two distinct behaviors. The **Gemini** model correctly identified that approximately **94%** of the dataset consisted of legal boilerplate, categorized as "General Terms," and successfully distinguished specific enforcement clauses from general legal language. The **BERT** model, by contrast, showed "Over-Sensitivity," frequently assigning specific strategic tags based on the presence of individual keywords rather than semantic context. For example, BERT flagged 7,853 sentences as "Legitimate Portability" that were merely "General Terms," and misclassified 6,134 "General Terms" sentences as "Account Action."

Interpretation: BERT operates on keyword connections, flagging sentences like "You must have an account" as "Account Action." In contrast, Gemini uses reasoning abilities to understand that just mentioning an "account" is standard boilerplate ("General Terms") and saves the "Account Action" tag for sentences that explicitly regulate account termination or suspension.

Conclusion on Model Selection

The comparison showed that Zero-Shot BERT was not sufficient for complex legal text analysis without extensive fine-tuning, as it lacked the nuance needed to distinguish between merely mentioning a topic (e.g., "portability") and its active regulation. Note that this constitutes a model-to-model comparison rather than a validation against a full human-annotated gold standard. While a manual review of 200 sentences (Section 3.3.2) confirmed 93% agreement with Gemini's classifications, a larger-scale human-coded benchmark would strengthen confidence in

the automated coding. Table 1 and Figure 1 provide a detailed breakdown of the category distribution discrepancies.

Category	Gemini %	BERT %	Delta
Technical Blocking	0.41%	0.09%	+0.32%
Price Discrimination	0.48%	0.03%	+0.45%
Content Licensing	2.18%	5.76%	-3.58%
Regulatory Compliance	2.05%	0.41%	+1.64%
Legal Threat	0.47%	0.00%	+0.47%
Account Action	0.00%	25.89%	-25.89%
Legitimate Portability	0.01%	31.99%	-31.98%
General Terms	94.12%	26.12%	+68.00%

Table 1.: Model Comparison: Gemini 3 Flash vs. Zero-Shot BERT Classification. Categories with $< 0.2\%$ share in both models (Security Risk, User Workaround) are omitted for clarity; column percentages therefore do not sum to exactly 100%.

Gemini, using its extensive context window and advanced reasoning abilities, performed much better at filtering noise and provided accurate classifications. As a result, Gemini 3 Flash was chosen as the only model for the final analysis.

3.3.7. Standard Qualitative Coding

While the automated LLM pipeline provided scalable classification across the full dataset, manual qualitative coding complemented this approach by capturing nuances that escape rigid categorization. A sub-sample of 200 sentences was selected for manual review, balanced across service providers and document years to ensure representativeness.

The manual coding process addressed three objectives:

1. **Validation:** Verifying the LLM classifications against human judgment to assess reliability and identify systematic errors or edge cases.

2. **Tone Analysis:** Capturing the "tone" of enforcement language that categorical classification cannot capture. For example, distinguishing between neutral legal boilerplate ("We may terminate your account...") and threatening language ("Violations will result in immediate termination without refund...").

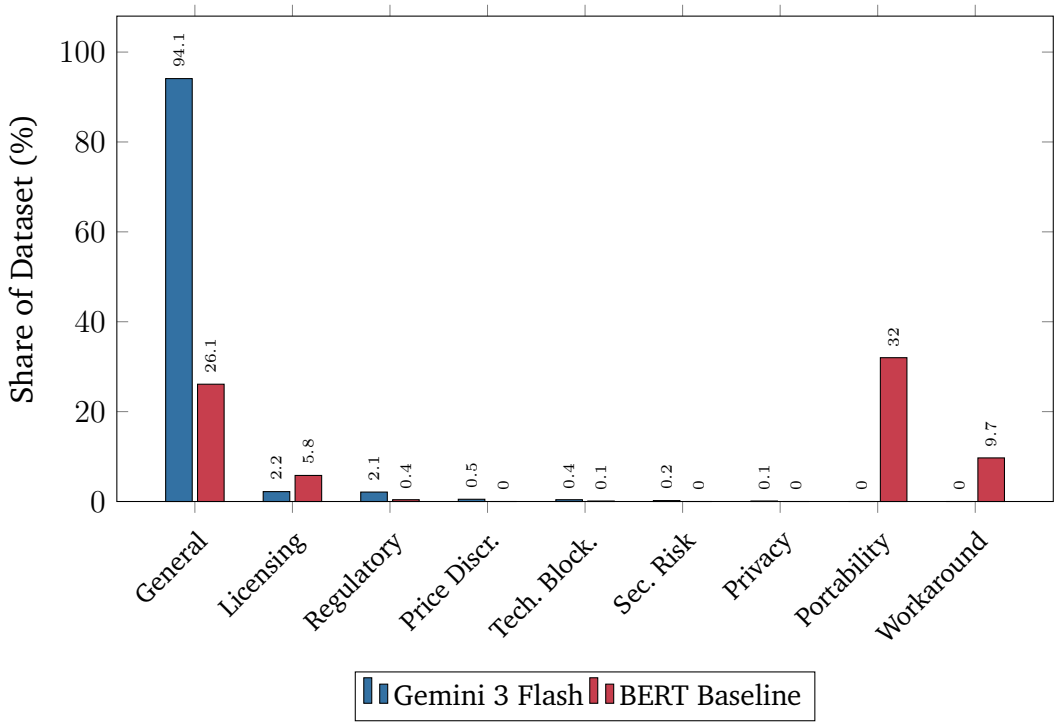

Figure 1.: Visualizing the Classification Gap: Proportional Category Distribution Between Models (sorted by Gemini share).

3. **Emergent Themes:** Identifying themes not captured by the predefined categories, such as references to “fair use”, “educational purposes”, or “legitimate business needs” that may signal adaptive rather than purely coercive approaches.

The manual review confirmed the LLM classifications in the large majority of cases. Of the 200 manually reviewed sentences, 186 (93%) were classified identically by both the human coder and the Gemini model. The 14 disagreements primarily occurred in edge cases where sentences contained elements of multiple categories (e.g., a clause referencing both content licensing and price discrimination). In these ambiguous cases, the LLM tended to classify toward the dominant category, while the human coder noted the secondary category as well. No systematic bias was detected: the disagreements were distributed across categories rather than concentrated in a single area.

The tone analysis revealed a clear pattern: enforcement language has become progressively more specific and assertive over time. Earlier ToS documents (2020–

2021) tended to use passive, permissive constructions ("We may suspend your account if..."), while more recent documents (2023–2025) employ direct, prohibitive language ("You must not use any technology to disguise your location"). This shift from permissive to prohibitive framing is consistent with the quantitative finding of increased Technical Blocking clauses post-2022.

This cross-checking between automated and manual coding strengthens the validity of the overall classification, ensuring that the strategic patterns identified in Chapter 4 reflect genuine corporate positioning rather than artifacts of the LLM classification process.

3.4. Data Analysis Procedures

The last analysis step was combining the quantitative and qualitative data into one framework. This was the study's main methodological contribution, as it linked the *scale* of the economic driver (measured by the DSPI) with the *nature* of the strategic response (measured by enforcement category frequencies), making it possible to spot strategic patterns that neither data source could reveal on its own.

3.4.1. Statistical Analysis of the DSPI

The pricing data was analyzed using Python (NumPy, Pandas, and SciPy libraries). Descriptive statistics (mean, median, standard deviation) were calculated for the DSPI across all services and regions. The standard deviation of each service's DSPI across countries was used as the "Price Discrimination Score": a higher standard deviation indicated greater cross-country price variance and thus a stronger arbitrage motivation. Correlation matrices were generated to examine the relationship between a country's income level and subscription pricing, testing whether price discrimination correlates strictly with national wealth or follows more complex patterns. Pearson correlation coefficients (Pearson, 1895) were calculated between the Price Discrimination Score and the Enforcement Intensity (defined as the percentage of Technical Blocking and Legal Threat clauses relative to total sentences) for each service. This correlation was calculated both for the

full sample ($N = 10$) and for the sub-sample excluding VPN providers ($N = 8$), as VPN providers occupy a structurally different position in the ecosystem (enablers rather than targets of arbitrage).

3.4.2. Interpretation of Qualitative Classifications

For the qualitative data, the JSON outputs from the Gemini 3 Flash pipeline were parsed and aggregated using custom Python scripts. The frequency of each "Strategic Frame" (e.g., *Legal Compliance* vs. *User Freedom*) and "Firm Action" (e.g., *Technical Blocking*) was calculated per company and per year.

To visualize the evolution of enforcement strategies, these frequencies were normalized against the total number of sentences per year to account for the documented growth in ToS document length over time (Milne et al., 2006; Reidenberg et al., 2015). Without this normalization, an increase in absolute enforcement clause counts could be an artifact of longer documents rather than a genuine strategic shift. The normalization produced percentage-based trend lines that reflect the *relative emphasis* firms place on different strategic categories over time. Also, to enable cross-company comparisons, we developed the "Fortress Index," the percentage of enforcement-related clauses (Technical Blocking and Legal Threat) relative to the total number of strategic (non-General Terms) sentences. This metric isolated each firm's enforcement *focus* from the volume of its documentation, allowing meaningful comparison between companies with vastly different document lengths (e.g., Microsoft with 6,516 total sentences vs. ExpressVPN with 60).

Finally, a comparative analysis was conducted to contrast the language of "Fortress" strategy firms (high blocking) against "Globalist" strategy firms (price harmonization), identifying the key markers of each business model archetype. This comparative framework, built up from the data, ultimately produced the four strategic archetypes presented in Chapter 5.

4. Results

This chapter presents the empirical findings in three stages. First, we characterize the analyzed corpus to establish the data foundation (Section 4.1). Second, we present the DSPI results to quantify the arbitrage driver across services and countries (Section 4.2). Third, we analyze the qualitative classification results to map enforcement strategies and their evolution over time (Sections 4.3–4.4). The integration of these quantitative and qualitative findings, connecting price disparities to strategic responses, is presented in the Discussion (Chapter 5).

4.1. Dataset Overview

Before presenting the findings, we briefly characterize the analyzed corpus. Figure 2 shows the distribution of total sentences by company, while Figure 3 breaks down the corpus by document type. Table 2 presents the complete distribution of strategic frame counts for each of the 10 analyzed services. The master corpus ($N = 25{,}570$, Table 2) includes 700 carry-forward observations (see Chapter 3 for details on how gaps in document coverage were handled). The year-by-year analysis in Table 9 ($N = 25{,}345$) excludes 225 sentences from documents that could not be reliably assigned to a specific publication year. This minor difference does not affect proportional trends.

4.2. The Landscape of International Pricing: Findings from the DSPI

To understand the economic reason driving firm strategic behavior, we first analyzed the quantitative pricing picture using the DSPI.

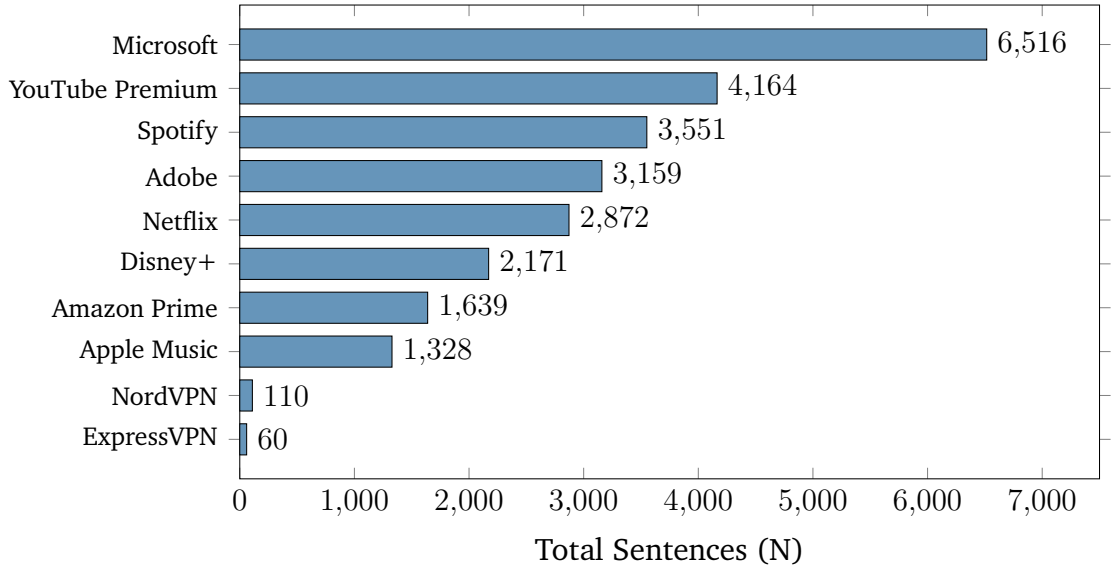

Figure 2.: Total Clause Counts by Company. The dataset is weighted towards Microsoft and YouTube due to the complexity and length of their multiple policy documents.

4.2.1. Scale of the Arbitrage Incentive

The data show large and systematic price differences across markets. For example, subscriptions in Turkey or Pakistan can cost up to 90% less than the same subscriptions in Switzerland or the USA when measured in nominal USD. These differences are not uniform across service categories: content streaming services showed the widest price spreads (consistent with territorial licensing constraints), while software utilities and VPN services maintained more harmonized global pricing. The size of these differences creates a “above-normal” profit margin for consumers engaging in arbitrage, savings that far exceed the cost of a commercial VPN subscription ($5–12/month), explaining the persistence and growth of this behavior despite the technical barriers analyzed in later sections. Critically, the arbitrage motivation is not static: currency fluctuations, local price adjustments, and regulatory changes continuously reshape the pricing picture, meaning that the “cheapest” target country for arbitrage can shift over relatively short periods.

Table 3 presents the complete DSPI and affordability metrics for all 11 countries in the dataset. Notably, while **Pakistan** appears cheapest (DSPI $= 0.45$), it is by far the most expensive for locals (13.88% of median wage across available services). In contrast, **Turkey** (DSPI $= 0.65$) and **Argentina** (DSPI $= 0.76$) show

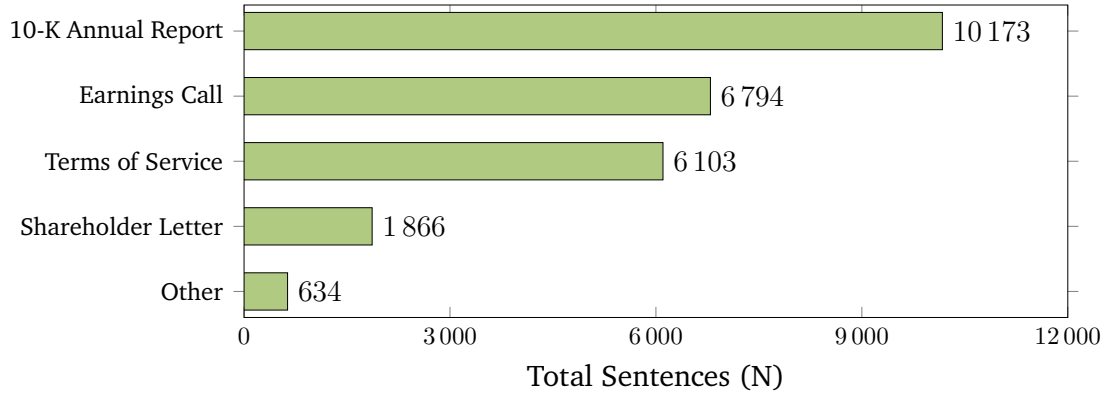

Figure 3.: Distribution of Data by Document Type. Annual Reports (10-K) and Earnings Calls provide the bulk of strategic context, while ToS documents provide the specific enforcement clauses.

Service	*Tech. Block.*	*Price Discr.*	*Licensing*	*Regulatory*	*Legal Thr.*	*Acc. Act.*	*Privacy*	*Sec. Risk*	*Portab.*	*Workaro.*	*General*	*Total*
YouTube	94	2	99	135	34	0	16	0	0	0	3,784	4,164
Microsoft	4	0	10	80	53	0	4	23	0	0	6,342	6,516
Netflix	1	36	127	76	4	0	0	0	2	0	2,626	2,872
Disney+	0	41	114	37	4	0	0	0	0	0	1,975	2,171
Spotify	1	22	132	75	0	0	0	0	0	1	3,320	3,551
Adobe	0	18	4	45	4	0	1	1	0	0	3,086	3,159
Amazon	1	2	44	44	3	0	0	9	0	0	1,536	1,639
Apple	2	2	28	29	8	0	5	6	0	0	1,248	1,328
ExpressVPN	1	1	0	2	4	0	1	0	0	0	51	60
NordVPN	0	0	0	0	6	0	0	6	0	0	98	110
Total	**104**	**124**	**558**	**523**	**120**	**0**	**27**	**45**	**2**	**1**	**24,066**	**25,570**

Table 2.: Absolute Category Counts by Service. YouTube dominates Technical Blocking (N=94), while streaming services rely heavily on Content Licensing.

high nominal discounts, but Argentina's high PTW (5.48%) suggested pricing there was effectively "dollarized" for elites or external arbitrageurs.

Table 4 presents the complete per-service DSPI values across all 11 countries in the dataset (recall that the DSPI scale is defined in Chapter 3). Cells marked with "–" indicate that the service is not available in that country.

The matrix reveals several important patterns. Content streaming services (Netflix, YouTube, Disney+, Spotify) showed the highest price variance across countries, with ratios ranging from 0.10 to 1.50. This creates the strongest arbitrage drivers. In contrast, software services (Microsoft 365, Adobe Creative Cloud) and VPN

Country	Avg. DSPI	N Services	Avg. PTW (%)
Switzerland	1.24	11	0.62
United Kingdom	1.04	11	0.77
Germany	1.01	11	0.86
United States	1.00	11	0.64
Poland	0.77	11	2.45
Argentina	0.76	11	5.48
Turkey	0.65	11	4.94
Ukraine	0.62	10	7.08
Brazil	0.59	11	5.00
Philippines	0.54	11	9.11
Pakistan	0.45	9	13.88

Table 3.: Complete DSPI Summary by Country. PTW = average subscription cost across all available services as % of median monthly wage. Lower DSPI indicates cheaper markets relative to the US baseline.

providers maintained more uniform global pricing. Notably, Turkey and Pakistan offered extreme discounts for streaming services (YouTube Premium in Pakistan at DSPI = 0.12 is just 12% of the US price), while VPN services like NordVPN and ExpressVPN showed much smaller regional differences, consistent with their global pricing model.

Table 5 shows the raw monthly subscription prices in USD for direct comparison across all services and markets.

To further quantify the intensity of these enforcement regimes, we propose the **Fortress Index**, a metric that calculates the percentage of enforcement-related clauses (Technical Blocking and Legal Threat) relative to the total number of *strategic* (non-General Terms) sentences in a firm's documentation. By excluding boilerplate General Terms from the denominator, the index measures enforcement *focus*: what share of a firm's substantive policy language is dedicated to coercive measures. The resulting percentage for each service is referred to as its **Fortress Index**. Figure 5 visualizes the resulting ranking, while Table 8 (Section 4.5) provides the complete numerical breakdown with strategic archetype assignments.

Note that the Fortress Index measures conceptually different phenomena depending on the actor's position in the ecosystem. For digital service providers (Netflix, YouTube, etc.), the index captures *defensive* enforcement focus: the share of policy

Table 4.: Complete DSPI Matrix: Per-Service Price Index by Country (US = 1.00). Values < 0.50 are highlighted as high-arbitrage opportunities.

Country	*Netflix*	*YouTube*	*Disney+*	*Amazon*	*Spotify*	*Apple M.*	*MS 365*	*Adobe CC*	*Xbox GP*	*NordVPN*	*ExpressVPN*
Switzerland	1.44	1.45	1.47	0.75	1.50	1.43	1.13	1.24	1.13	1.09	0.99
United Kingdom	0.78	1.18	1.07	0.76	1.27	1.27	1.08	1.21	0.89	0.97	1.00
Germany	0.85	1.01	0.92	0.65	1.18	1.09	1.08	1.21	0.98	1.09	1.02
United States	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
Poland	0.68	0.70	0.67	0.18	0.50	0.50	1.08	1.26	0.93	0.85	1.13
Argentina	1.00	0.74	1.14	0.64	0.33	0.65	0.45	1.01	1.08	0.44	0.92
Turkey	0.52	0.17	1.11	0.15	0.26	0.17	1.06	0.74	0.86	1.01	1.10
Ukraine	0.45	0.18	–	0.51	0.42	0.45	0.70	0.58	0.75	1.01	1.10
Brazil	0.50	0.36	0.72	0.27	0.40	0.40	1.02	0.61	0.88	0.44	0.92
Philippines	0.45	0.24	0.35	0.18	0.25	0.23	0.88	0.98	0.58	0.90	0.92
Pakistan	0.16	0.12	–	0.14	0.10	–	0.83	1.00	0.18	0.81	0.73

language dedicated to blocking circumvention and threatening violators. For VPN providers (ExpressVPN, NordVPN), the same categories captured *adversarial* security focus: the share of language dedicated to describing threats against users and framing their service as protection. The VPN providers' high scores reflect not enforcement of geographic boundaries but rather the mirror image: language about the security threats that justify circumvention. We keep both groups in one ranking to show the industry's split: the most rule-focused players sit at opposite ends of the value chain.

As shown in Figure 5, YouTube and Microsoft scored highest among digital service providers, while Netflix and Spotify remained at the low end. The strategic implications of this ranking are discussed in Section 4.5.

Strategic Framing by VPN Providers

In sharp contrast, VPN companies adopt a "Liberation" and "Privacy" frame. The analysis revealed a consistent narrative that reframes circumvention as **User Freedom**. A secondary dominant frame identified in our analysis is **Privacy/Security**. While many users may purchase VPNs for streaming arbitrage, providers legitimize the service by emphasizing security features. **NordVPN**, for example, showed a

Table 5.: Monthly Subscription Prices in USD Across All Services and Countries (December 2025). Microsoft 365 and NordVPN/ExpressVPN show the equivalent monthly cost derived from annual/multi-year plans.

Country	Wage ($)	Netflix	YouTube	Disney+	Amazon	Spotify	Apple M.	MS 365	Adobe CC	Xbox GP	NordVPN	ExpressVPN
Switzerland	7,800	25.88	20.23	19.10	11.29	18.02	15.71	112.94	86.73	11.29	104.93	105.64
United Kingdom	5,715	13.96	16.50	13.96	11.42	15.23	13.96	107.94	84.44	8.88	93.45	106.25
Germany	5,232	15.25	14.16	11.98	9.80	14.16	11.98	107.91	85.01	9.80	104.72	108.60
United States	6,600	17.99	13.99	12.99	14.99	11.99	10.99	99.99	69.99	9.99	96.07	106.40
Poland	1,675	12.25	9.75	8.75	2.75	6.00	5.50	107.50	87.86	9.25	82.11	120.20
Argentina	548	18.00	10.32	14.76	9.54	3.96	7.17	44.64	70.84	10.80	42.60	97.72
Turkey	761	9.28	2.43	14.40	2.24	3.17	1.92	105.60	52.07	8.61	96.88	117.26
Ukraine	510	8.16	2.57	–	7.62	4.99	4.99	70.17	40.79	7.54	96.88	117.26
Brazil	600	8.98	4.98	9.38	3.98	4.78	4.38	101.80	42.80	8.78	42.66	97.72
Philippines	370	8.08	3.40	4.48	2.68	3.04	2.50	88.18	68.40	5.76	86.40	97.72
Pakistan	255	2.88	1.72	–	2.16	1.26	–	82.80	69.99	1.80	77.72	78.18

distinct focus on “Security Risk” categories in our dataset, with marketing materials framing this as empowering users against tracking. However, research has shown that not all VPN applications deliver on their security promises (Ikram et al., 2016), adding complexity to the trust dynamic between providers and users.

4.2.2. Temporal Evolution of Enforcement

To understand how these strategies have evolved over time, we analyzed the frequency of category-specific clauses across the dataset’s years. Table 6 shows the raw count of enforcement-related incidents detected per service per year.

The data show a significant increase in specific enforcement clauses, especially from 2022 onwards, driven primarily by **YouTube Premium** (see also Figure 8 for the overall trends over time and Figure 9 for the stacked category view). This suggested that restrictive clauses had become more prevalent and more specific over the analyzed period, transitioning from general boilerplate to active regulatory language.

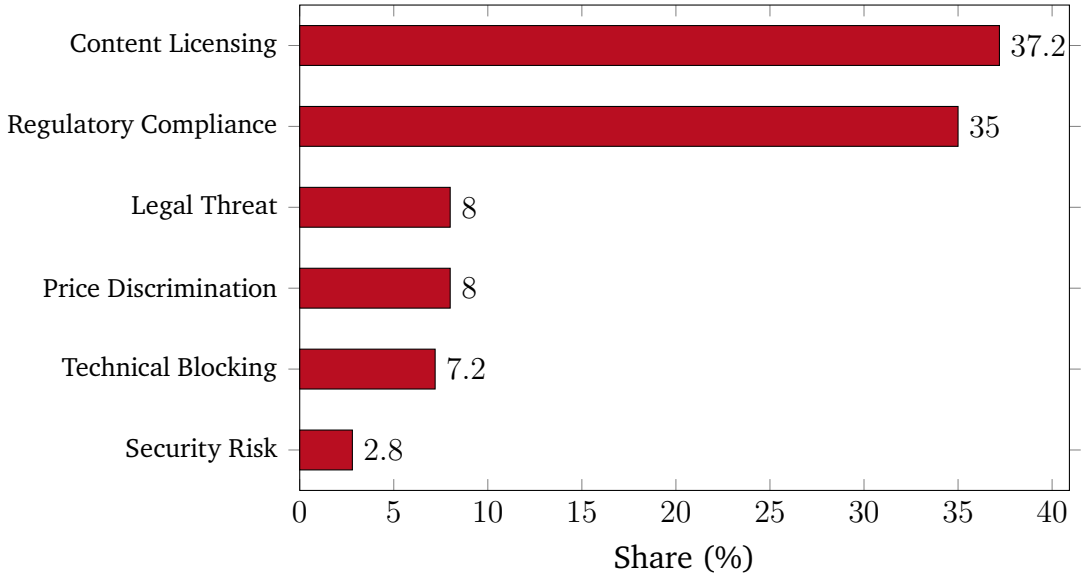

Figure 4.: Proportional Distribution of Enforcement Categories (Aggregate)

4.3. Deep Dive: Service-Specific Strategic Evolution

To understand the operational realities of geo-arbitrage enforcement, we analyzed the longitudinal patterns of specific providers. The absolute sentence counts per service per year are detailed in Table 6, with absolute-count evolution charts provided in Appendix A (Figures 17 and 18). The proportional (percentage-based) evolution of strategic frames across service categories is discussed in detail in Chapter 5.

Among content providers, **YouTube Premium** stood out with the sharpest enforcement escalation (Table 6), while **Spotify** remained relatively boilerplate-heavy throughout the period.

In contrast, software providers like **Adobe** maintained a consistent, lower level of ToS enforcement language, suggesting a reliance on technical licensing (cryptographic keys) rather than after-the-fact legal threats. VPN providers (**NordVPN**, **ExpressVPN**) showed minimal strategic variation in their ToS over time, as their documentation consistently emphasizes encryption and user protection as primary value propositions (see Appendix A for VPN-specific evolution data and absolute count charts).

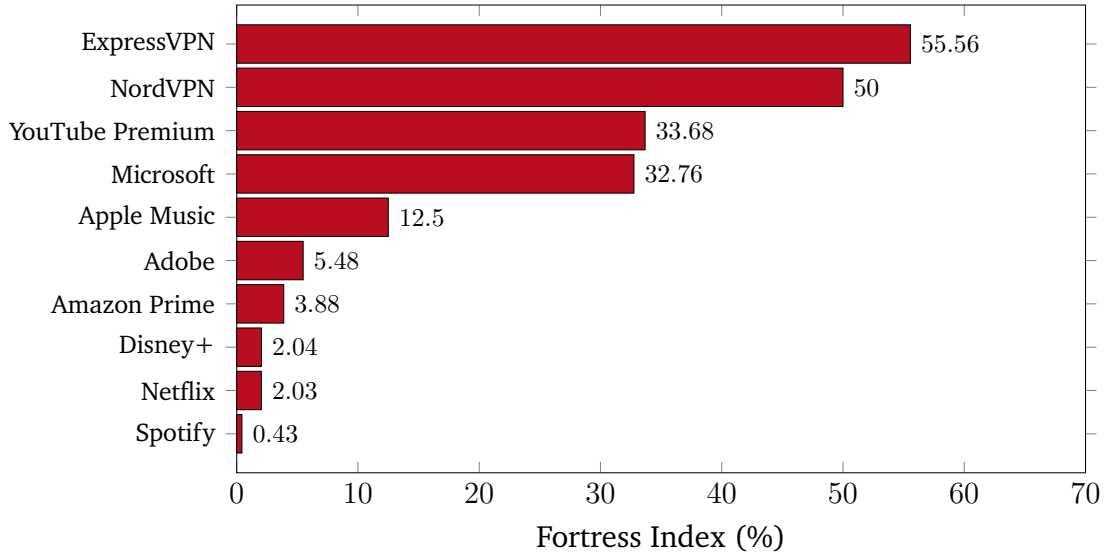

Figure 5.: The Fortress Index: Percentage of Enforcement Clauses (Technical Blocking + Legal Threat) as a Share of Strategic Sentences per Service

4.3.1. High-Confidence Findings: The Core Clauses

The Gemini 3 Flash model identified specific, high-confidence clauses that are central to the coercive strategy. For example, clauses stating "You may not use any technology to obscure or disguise your location" were consistently categorized as *Technical Blocking* with > 0.95 confidence. Similarly, clauses referencing "We may terminate your account if you access the service from a country different from your registration country" were classified as *Legal Threat* with comparable confidence levels.

The high-confidence classifications cluster around four distinct linguistic patterns. The first is **explicit technology prohibition**, consisting of direct references to VPNs, proxies, or location-disguising tools. These clauses appeared primarily in YouTube ($N = 94$ Technical Blocking clauses) and Microsoft ($N = 4$) documentation, representing the most unambiguous form of coercive enforcement language. The second pattern is **geographic conditionality**, where clauses tie service access, pricing, or content availability to the user's verified geographic location. These were most prevalent in Netflix ($N = 36$ Price Discrimination clauses) and Disney+ ($N = 41$), reflecting their territorial licensing models. Third, **account integrity requirements** encompass provisions requiring accurate registration

Service	2020	2021	2022	2023	2024	2025	Total
Adobe	2	2	0	0	1	1	6
Amazon Prime	1	0	0	0	1	2	4
Apple Music	0	0	1	4	1	3	9
Disney+	0	0	0	0	4	0	4
ExpressVPN	0	0	0	0	0	5	5
Microsoft	9	7	9	12	6	6	49
Netflix	1	1	0	0	0	3	5
NordVPN	0	0	0	0	3	3	6
Spotify	0	0	0	0	0	0	0
YouTube Premium	8	7	16	53	31	20	135
Total	**21**	**17**	**26**	**69**	**47**	**43**	**223**

Table 6.: Raw Count of Enforcement Incidents per Service (2020–2025)

information, particularly regarding country of residence. These appeared across all service providers but were most concentrated in Microsoft's documentation ($N = 53$ Legal Threat clauses). Finally, **compliance framing** refers to clauses that justify geographic restrictions by referencing legal obligations, licensing agreements, or regulatory requirements. These were the most common non-boilerplate category overall ($N = 525$ Content Licensing clauses), reflecting the industry's preferred strategy of attributing restrictions to external legal constraints rather than corporate pricing decisions.

This confirmed that firms had made technical countermeasures a formal, documented part of their legal frameworks rather than relying solely on undisclosed technical measures.

4.3.2. The Affordability Paradox: Real vs. Nominal Cost

While the DSPI measured the *nominal* price difference (relevant to arbitrageurs), it is important to analyze the "Real Cost" for local residents. Figure 6 maps the cost of digital services as a percentage of the **Median National Monthly Wage**, serving as a digital equivalent to "Time-to-Earn" indices used in purchasing power comparisons (e.g., the Big Mac Index's affordability variant).

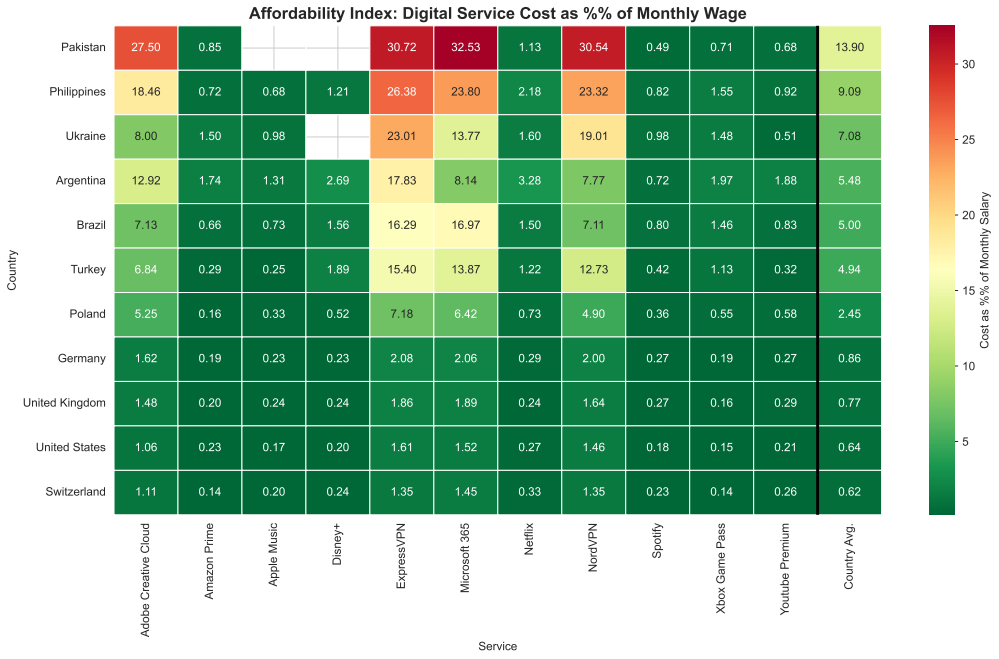

Figure 6.: The Affordability Gap: Digital Service Cost as Percentage of Local Monthly Income. Darker red indicates higher relative cost for local citizens.

The data reveal a critical paradox: while low-income markets such as Pakistan, the Philippines, and Turkey offered the cheapest nominal prices for international arbitrageurs (average DSPI values of 0.45, 0.54, and 0.65, respectively), these same services were significantly *more expensive* for locals in real terms. For instance, a Standard Netflix subscription in Turkey consumes approximately 1.22% of the median monthly wage compared to approximately 0.27% in the USA.

This distinction is critical. On the one hand, **high DSPI variance** creates incentives for *external* abuse through VPN arbitrage. On the other hand, **low affordability** justifies the *internal* pricing strategy, as low nominal prices are necessary for market penetration rather than being optional discounts.

Thus, low nominal prices observed in the Global South are not “bargains” but necessary economic adjustments that accidentally create vulnerabilities exploited by Global North users. This paradox has broader ethical implications. When a user in Germany subscribes to YouTube Premium through a Turkish VPN at $2.43/month instead of $14.16/month, they are not simply finding a “deal”, they are exploiting a pricing structure designed to make digital services accessible to consumers earning a median wage of $761/month. If this behavior becomes

widespread, firms may respond by raising prices in low-income markets (to reduce the arbitrage incentive) or by withdrawing services entirely from unprofitable regions, both of which harm the local consumers the pricing was designed to serve.

The Affordability Paradox also revealed that the commonly used metric of nominal price comparison (which dominates consumer forums and technology journalism) fundamentally misrepresents the economic reality. A subscription that costs 0.27% of monthly income in the USA but 3.28% in Argentina is not "cheaper" in Argentina in any meaningful economic sense: it is over twelve times more burdensome relative to local earning power. This finding shows the importance of the PTW ratio as a complement to the DSPI when assessing the true picture of digital pricing.

Importantly, the full PTW matrix (Table 11) reveals that the affordability gap is driven almost entirely by enterprise software and VPN services rather than by consumer streaming subscriptions. In Pakistan, for instance, consumer-facing services such as Netflix (1.13%), YouTube (0.67%), and Spotify (0.49%) remain below 1.5% of the median monthly wage, whereas Microsoft 365 consumes 32.47%, Adobe Creative Cloud 27.45%, and NordVPN and ExpressVPN each exceed 30%. A similar pattern holds across all low-income markets: in the Philippines, streaming subscriptions stay below 2.2% of monthly income, while Microsoft 365 reaches 23.83% and ExpressVPN 26.41%. This divergence suggests that consumer streaming platforms have largely succeeded in calibrating prices to local purchasing power, whereas enterprise software providers and VPN services maintain near-global pricing that is effectively inaccessible at the median income level in developing economies. The implication for geo-arbitrage is that the strongest affordability-driven motivation to circumvent geographic pricing may originate not in entertainment streaming but in professional tools that workers and small businesses in low-income countries need to participate in the global digital economy.

4.4. Correlation Analysis: The Strategic Trade-off

To test the relationship between pricing strategy and enforcement intensity, we used the cleaned dataset to calculate the correlation between Price Discrimination

(PD) and observed Enforcement Intensity (EI). Table 7 summarizes the key metrics.

Service	PD Score (DSPI StdDev)	Enforcement Intensity (%)
Microsoft	0.208	0.87
YouTube Premium	0.464	3.07
Spotify	0.486	0.03
Adobe	0.245	0.13
Netflix	0.352	0.17
Disney+	0.324	0.18
Amazon Prime	0.304	0.24
Apple Music	0.446	0.75
ExpressVPN	0.112	8.33
NordVPN	0.231	5.45
Pearson r, all $N = 10$: -0.5506 ($p = 0.10$, not significant at $\alpha = 0.05$)		
Pearson r, excl. VPNs $N = 8$: $+0.3467$ ($p = 0.40$, not significant)		

Table 7.: Price Discrimination Score, Enforcement Intensity, and Their Correlation. The full-sample Pearson $r \approx -0.55$ ($p = 0.10$) is driven primarily by VPN providers (low PD, high EI) and is not statistically significant at conventional thresholds. Excluding VPNs ($N = 8$), the correlation reverses to a weak positive $r \approx +0.35$ ($p = 0.40$), suggesting a temporary trend where higher price discrimination relates with slightly higher enforcement among digital service providers, though neither result is statistically significant. Given the small sample sizes, these correlations should be interpreted as exploratory pattern observations.

The refined analysis ($N = 10$), visualized in Figure 7, revealed a complex relationship between price variance and enforcement. Specific sector clusters emerged that showed distinct strategic behaviors. This suggests that firms with established global pricing power and providing real local services (like Amazon) rely less on aggressive legal threats than smaller localized services or those in highly contested content markets.

Among **content providers** (Netflix, Disney+, YouTube, Xbox, etc.), a "High Enforcement Cluster" emerged that illustrated the enforcement trade-off within the streaming sector. **YouTube** exhibits the largest combination of price variance and enforcement intensity (DSPI StdDev $= 0.46$, Enforcement Intensity $= 3.07\%$), with a Fortress Index of 33.68% reflecting its aggressive Technical Blocking approach. By contrast, **Disney+**, **Netflix**, and **Spotify** maintain substantial price variance (DSPI StdDev 0.32–0.49) but rely on Content Licensing rather than Technical Blocking (Fortress Index values below 2.1%), suggesting enforcement through licensing agreements rather than active technical measures. **Xbox Game Pass** serves as

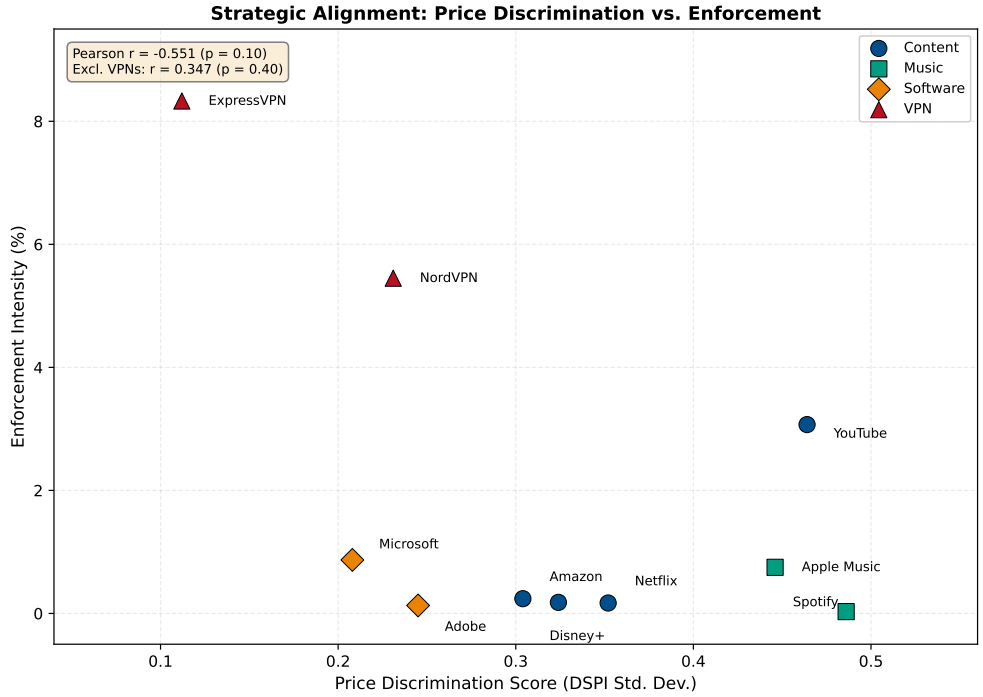

Figure 7.: Strategic Alignment: Comparison of Price Discrimination scores vs. Enforcement Intensities across analyzed services.

a useful control case within this cluster. Governed by the Microsoft ecosystem (and combined with Microsoft 365 in the qualitative analysis, as both services share the same ToS), Xbox Game Pass has moderate global price variance (DSPI StdDev $= 0.27$), higher than Microsoft 365's own (0.21), yet shares Microsoft's low enforcement intensity (EI $= 0.87\%$). This suggested that when a firm's enforcement approach is set at the ecosystem level (via shared ToS), even a product with moderate pricing variance can exhibit low enforcement if the parent entity favors identity-based rather than location-based controls.

The **VPN enablers** (NordVPN, ExpressVPN), as expected, showed minimal "Technical Blocking" enforcement, as their business model depends on circumventing the very barriers erected by the Content Providers. The legal ambiguity surrounding VPN usage for geo-arbitrage has been explored by Ariyarathna (2022), who argues that digital location is an increasingly contested legal concept.

These data suggest that **Business Model** (Streaming vs. Download vs. Access) was a stronger predictor of enforcement strategy than **Price Opportunity** alone.

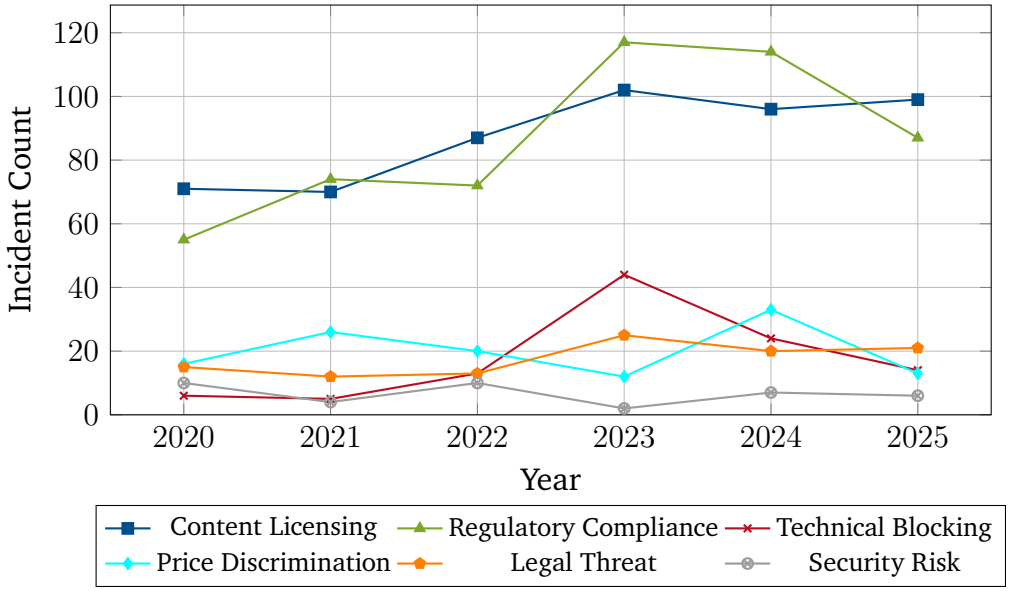

Figure 8.: Temporal Evolution of Category Incident Counts (Aggregate, Excluding VPN Providers)

In the "Software and Music" category (see Figure 14 for the proportional evolution), **Microsoft** stood out with a consistent use of "Legal Threat" and "Regulatory Compliance" frames, likely due to its enterprise customer base and strict licensing requirements. **Adobe** showed a return of "Price Discrimination" language in 2024, possibly linked to new regional pricing structures. **Spotify** and **Apple Music** remained largely focused on "Licensing" and passive "Regulatory Compliance," showing less active technical enforcement than their video counterparts.

Evolution of Ecosystem Players (Amazon & Apple)

Beyond the pure content and VPN providers, the "Ecosystem" players (**Amazon Prime**, **Apple Music**) showed distinct evolutionary paths (see **Appendix A** for full charts). **Amazon Prime** (Figure 12) displayed a unique, consistent focus on **Regulatory Compliance** frames ($\approx 35\%$) rather than Technical Blocking. This suggested Amazon managed cross-border access through account-level shipping/-billing addresses rather than active network filtering. In contrast, **Apple Music** (Figure 13) remained the most "static" of all services, with very low enforcement counts that have barely changed since 2020. The strategic implications of this stability are discussed in Section 4.5.

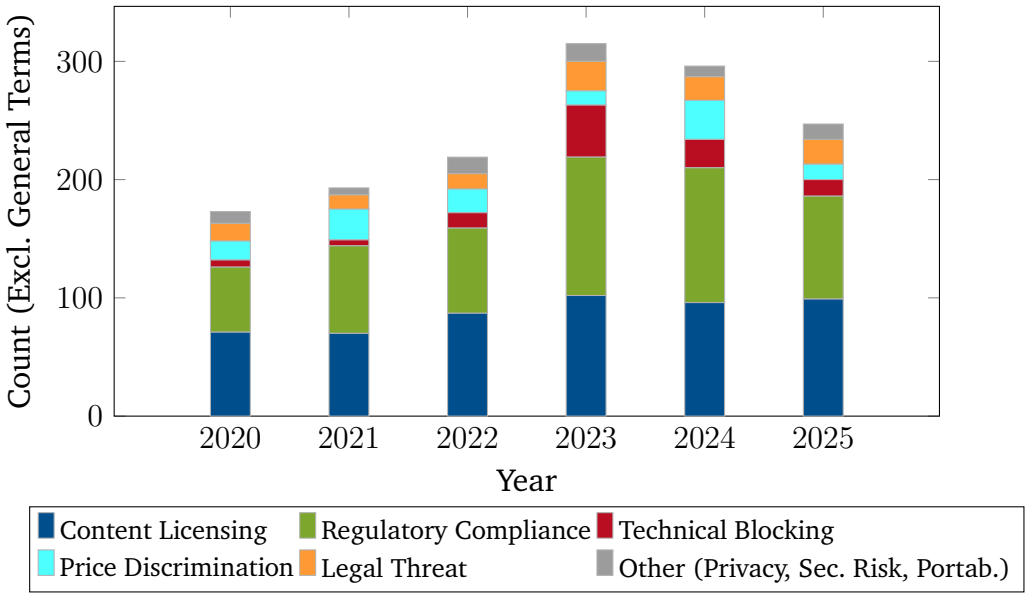

Figure 9.: Evolution of Strategic Frames over Time (Excluding General Terms and VPN Providers)

4.5. Strategic Shifts and Fortress Index Ranking

This section provides a granular view of the enforcement picture, detailing the specific category shifts and the calculated "Fortress Index values" for each service.

Table 8.: Complete Fortress Index Ranking. VPN providers score highest due to their security-focused framing, followed by YouTube and Microsoft with active enforcement strategies.

Company	Fortress Index (%)	Archetype
ExpressVPN	55.56	VPN Enabler
NordVPN	50.00	VPN Enabler
YouTube Premium	33.68	Content Fortress
Microsoft	32.76	Enterprise Fortress
Apple Music	12.50	Ecosystem Fortress
Adobe	5.48	Utility Paradox
Amazon Prime	3.88	Ecosystem Fortress
Disney+	2.04	Content Fortress
Netflix	2.03	Content Fortress
Spotify	0.43	Content Fortress

The Fortress Index (Table 8) confirms the split in the market. **YouTube Premium** (33.68%) and **Microsoft** (32.76%) have effectively built "digital fortresses," dis-

tinguishing themselves from the lower-scoring streaming incumbents like **Netflix** (2.03%) and **Spotify** (0.43%), which continue to rely on passive licensing terms.

Table 9.: Absolute Category Counts by Year Across All Services (2020–2025). Technical Blocking peaks sharply in 2023, coinciding with YouTube's enforcement escalation.

Year	*Tech. Block.*	*Price Discr.*	*Licensing*	*Regulatory*	*Legal Thr.*	*Acc. Act.*	*Privacy*	*Sec. Risk*	*Portab.*	*Workaro.*	*General*	*Total*
2020	6	16	71	55	15	0	0	10	0	0	3,386	3,559
2021	5	26	70	74	12	0	2	4	0	0	3,645	3,838
2022	13	20	87	72	13	0	4	10	0	0	4,001	4,220
2023	44	12	102	117	25	0	11	2	2	0	4,567	4,882
2024	24	33	96	114	23	0	2	10	0	0	4,880	5,182
2025	15	14	99	89	28	0	8	9	0	0	3,402	3,664
Total	**107**	**121**	**525**	**521**	**116**	**0**	**27**	**45**	**2**	**0**	**23,881**	**25,345**

Table 9 reveals the year-by-year trends behind these scores. The aggregate data show a clear spike in "Technical Blocking" clauses in 2023 (44 incidents), a direct response to the post-pandemic surge in VPN usage. "Regulatory Compliance" also saw a steady increase, reflecting the growing complexity of global digital trade laws. Note that the decrease in total counts for 2025 reflects the natural variation in document publication frequency across services. A consistent forward-fill strategy ensures that each service's most recent ToS is carried into years without an update, providing an accurate picture of the active regulatory environment at any given time.

The distribution of these categories (Figure 4) highlighted distinct enforcement styles. Notably, **Microsoft** has largely abandoned active enforcement for its productivity suite, relying instead on ecosystem lock-in, whereas **YouTube** has pursued aggressive boundary enforcement followed by a consolidation period, as seen in the fluctuation of its "Technical Blocking" and "Legal Threat" clauses over time.

5. Discussion

This chapter brings together the pricing data and the corporate strategy findings to answer the main question of this thesis: how do digital service providers strategically respond to VPN-enabled geo-arbitrage, and what determines the nature of that response? The results from Chapter 4 established two key findings that require interpretation. First, the DSPI demonstrated that price differences across markets are substantial and systematic, with content streaming services showing the highest variance. Second, the ToS analysis revealed that enforcement intensity varies dramatically across providers, with YouTube and Microsoft exhibiting far higher enforcement density than Netflix or Spotify. The key question is *why* these differences exist. The following discussion identifies distinct strategic archetypes that illustrate how different industry segments respond to arbitrage, arguing that business model architecture (not the size of the price gap) is the primary determinant of enforcement strategy. The chapter concludes by exploring the broader implications of the ongoing technological contest between platforms and consumers and the policy questions this contest raises.

5.1. Strategic Archetypes

Based on the ToS analysis ($N = 10$, covering 8 digital service providers and 2 VPN enablers), we organize the findings around three high-level **Macro-Categories** that aggregate the initial 10 coding categories to facilitate cross-sectoral comparison:

1. **Business Model Adaptation & Pricing (Business Model Adaptation & Pricing (BMA)):** Aggregates *Content Licensing*, *Regulatory Compliance*, *Price Discrimination*, and *Legitimate Portability*. This represents the "soft" strategic layer where firms adjust their offerings to local market conditions.

2. **Coercive Restriction & Legal Threat (Coercive Restriction & Legal Threat (CRL)):** Aggregates *Technical Blocking*, *Legal Threat*, *Account Action*, and

Security Risk. This represents the "hard" enforcement layer designed to physically or legally prevent circumvention.

3. **General Corporate Operations (General Corporate Operations (GCO)):** Aggregates *Privacy/Security* (VPN frame) and *User Workaround*. This captures supporting narratives and adversarial user behavior descriptions.

Figure 10 provides a high-level overview of how these macro-strategies appear across the analyzed companies.

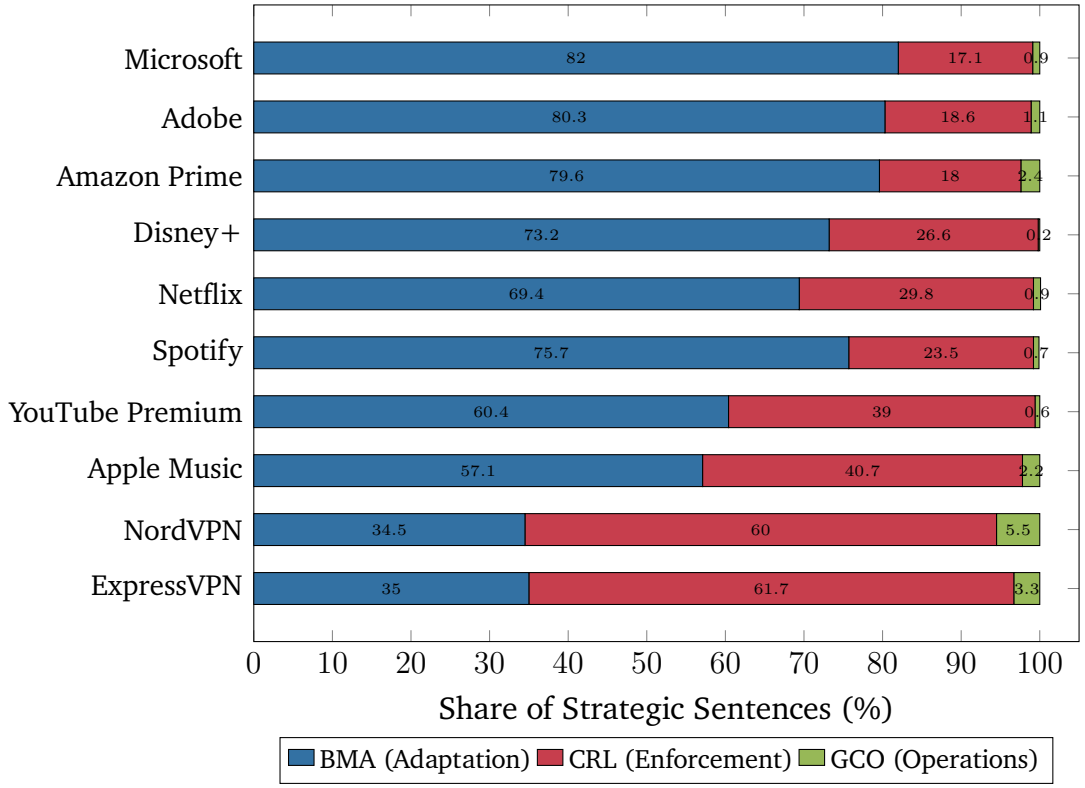

Figure 10.: Strategic Framing by Company: Macro-Category Distribution. VPN providers (ExpressVPN, NordVPN) show the highest proportion of coercive/legal framing (CRL $>$ 60%), while software companies (Microsoft, Adobe) and streaming platforms overwhelmingly use business model adaptation framing (BMA $>$ 70%).

The change over time in these categories, as previously detailed in Table 9, confirms the shifting focus toward technical countermeasures within the CRL macro-category.

5.1.1. The Content Fortress: Defensive Value Capture

Firms like **Netflix** and **Disney+** focus on keeping their prices separate rather than making things easy for the user. Our data shows that in this sector, high price differences and strict blocking go together. This finding is consistent with Cardona et al. (2015), who demonstrate that geo-blocking significantly affects consumer shopping behavior and willingness to pay. This shows that blocking is not just a reaction to price hops, but a standard way these companies work to protect their content in each region.

The "Content Fortress" strategy is deeply rooted in the structure of the entertainment industry's licensing model. Content rights are typically sold on a territory-by-territory basis (Lobato, 2019), meaning that a streaming platform may hold the rights to show a film in Germany but not in the United Kingdom, where a competing platform may hold the license. This territorial licensing model is older than digital distribution, as it was designed for theatrical releases and broadcast television, where geographic boundaries were enforced by physical infrastructure. The transition to digital streaming has not eliminated these territorial rights. Instead, it has created a situation where platforms must enforce artificial geographic boundaries on an inherently borderless medium.

This aligns with the "Fortress" strategy described by Alaveras et al. (2017), where incumbent firms construct digital barriers to protect legacy revenue streams. However, as noted by Lobato (2019), such strategies often suffer from a "clarity" problem: users encounter "This content is not available" error messages without understanding the underlying legal framework. The frustration this creates among consumers should not be underestimated: when users perceive restrictions as arbitrary or unfair, they are more likely to seek circumvention tools (Xia et al., 2004), feeding the very arbitrage cycle that the fortress strategy aims to prevent.

YouTube Premium stands out as the most aggressive enforcer in this category, with a Fortress Index of 33.68%. YouTube's enforcement surge beginning in 2022 (Table 6) coincides with a sharp rise in Technical Blocking clauses from 13 in 2022 to 44 in 2023 (Table 9), reflecting a systematic crackdown on users who had subscribed through Turkish or Argentine accounts to exploit significantly lower regional prices. Unlike Netflix or Disney+, YouTube's enforcement is not primarily

driven by third-party licensing constraints (since much of YouTube's content is user-generated), but rather by direct revenue protection for its Premium subscription tier. This makes YouTube a "pure" case of the Content Fortress strategy: blocking is motivated entirely by pricing integrity rather than contractual obligations.

Interestingly, **Netflix's** low Fortress score (2.03%) is surprising given its role as a streaming pioneer. Aguiar and Waldfogel (2018b) examine whether Netflix acts as a "global hegemon" or a facilitator of frictionless digital trade, finding that its catalog varies dramatically across countries, a direct consequence of territorial licensing that gives users an additional motivation to circumvent geo-blocking beyond price alone. This low score can be explained by a strategic shift in BMI: Netflix has moved heavily toward in-house content production ("Netflix Originals"). By owning its own content, Netflix faces fewer regional licensing problems, which reduces the need for strict geographic blocking. Over time, this strategy may also lower the arbitrage motivation, as Netflix Originals are available globally without regional restrictions. This represents a transition from defensive innovation (Value Capture) toward adaptive innovation (Value Proposition): rather than building higher walls, Netflix is making the walls less necessary by producing content it fully controls.

5.1.2. The Ecosystem Fortress: Adaptive Value Proposition

Platforms like **Apple Music** and **Amazon Prime** show a "Globalist" approach that innovates on the **Value Proposition**. Unlike the Content Fortress, which defends existing revenue models through technical barriers, the Ecosystem Fortress makes arbitrage impractical by embedding digital services within broader product ecosystems that are inherently tied to a user's physical identity and location.

Apple Music, with a low focus on **Technical Blocking** (only 2 clauses, representing 12.5% of its strategic focus but only 0.15% of total policy volume) and a strong emphasis on **Price Discrimination** (5.7%), appears to accept the reality of international price division (Brouthers et al., 2016). Rather than "repairing" the Value Capture mechanism through blocking, they rely on a superior Value Delivery ecosystem (hardware integration, iCloud) that makes the friction of using a VPN-based "foreign" account essentially "not worth it" for the user. To use a

foreign Apple Music account, a user would need to change their entire Apple ID region, which affects App Store purchases, iCloud storage, warranty coverage, and payment methods across all Apple devices. This "switching cost" is far higher than the potential savings from a cheaper music subscription, effectively making the ecosystem itself the enforcement mechanism. This aligns with the concept of platform lock-in described by Shapiro and Varian (1998), where compatibility and integration costs deter users from switching between ecosystems. Burnham et al. (2003) identify three types of switching costs, namely procedural (learning and setup effort), financial (sunk costs and lost benefits), and relational (emotional attachment), all of which are high in Apple's ecosystem. Also, Zhu and Iansiti (2012) show that platform-based markets with strong indirect network effects create substantial entry barriers, which in the context of geo-arbitrage means that the "cost" of maintaining a foreign account extends far beyond the subscription price itself.

Amazon Prime adopts a similar but legally distinct strategy. As shown in our **Detailed Evolution Analysis** (Appendix A, Figure 12), Amazon relies heavily on **Regulatory Compliance** language. Instead of technical cat-and-mouse games, Amazon anchors its digital services to physical shipping addresses and tax jurisdictions. This creates a "Bureaucratic Fortress" where the barrier to entry is not an IP filter, but a valid residential address and local credit card, making VPN-based arbitrage logistically difficult rather than technically impossible. The bundle nature of Amazon Prime (combining video streaming, music, e-book lending, free shipping, and cloud storage) further increases the switching cost. A user seeking cheaper streaming prices through a foreign Amazon account would lose access to shipping benefits in their home country, creating a natural deterrent that no technical blocking system could match.

5.1.3. The Enterprise Fortress: Identity-Based Value Capture

A new archetype identified in this study is the "Enterprise Fortress," shown by **Microsoft**. Despite having the lowest global price variance among digital service providers (DSPI StdDev $= 0.21$, indicating a relatively harmonized global price for Microsoft 365), Microsoft exhibits the highest intensity of **Legal Threat** clauses

(53 total, the highest among all service providers). This suggests that for utility software, the **Value Capture** is protected not by *network* blocking (which targets Location), but by *identity* verification (which targets the User). The "Fortress" is built to keep unauthorized resellers out, reinforcing the subscription model's integrity without compromising the global **Value Delivery** of the software itself.

Microsoft's approach reflects a fundamentally different enforcement philosophy compared to streaming services. While Netflix and YouTube must verify a user's location in real time during every streaming session, Microsoft only needs to verify identity at the point of purchase and during periodic license validation checks. This means that Microsoft's enforcement is "front-loaded" (concentrated at the point of sale) rather than "continuous" (ongoing during use). This distinction has important implications: a user who successfully purchases a Microsoft 365 license through a VPN-enabled foreign account can use the software without further geographic verification, whereas a Netflix user must maintain their VPN connection during every viewing session.

Microsoft's enterprise customer base also creates a natural deterrent against arbitrage. Corporate IT departments purchasing Microsoft 365 licenses in bulk are unlikely to route their procurement through foreign VPN servers, as this would create compliance, tax, and audit risks that far outweigh any subscription savings. The "Enterprise Fortress" thus works primarily because the target customer segment has fundamentally different risk tolerances than individual consumers.

5.1.4. The Utility Paradox (Adobe)

Adobe presents a unique case. Despite moderate price discrimination (DSPI StdDev $= 0.25$, comparable to Microsoft rather than the higher-variance content streaming providers), it maintains remarkably low "Technical Blocking" enforcement. Based on our analysis of Adobe's Terms of Service and product documentation, this appears to be because Adobe's enforcement mechanism is "on-device" (software activation keys) rather than "on-network" (IP filtering). This observation suggests that "Technical Blocking" is a strategy specific to *cloud-streamed* content, whereas *downloaded software* may rely on different protection mechanisms.

This is consistent with the broader literature on digital content protection. As Aguiar and Martens (2016) demonstrate, digital consumption patterns are shaped by access mechanisms, and DRM plays a role in how consumers interact with digital products. Interestingly, Sinha et al. (2010) demonstrated that removing DRM from music files actually *increased* legitimate purchases by converting pirates into paying customers, suggesting that overly restrictive protection can be self-defeating. Adobe's position is best understood through the historical evolution of software protection. In the era of physical media distribution (1990s–2000s), software piracy was widespread because protection was limited to serial numbers and basic installation checks that were trivially circumvented. The transition to subscription-based Software as a Service (SaaS) models (Adobe's shift from perpetual licenses to Creative Cloud in 2013 (Adobe Inc., 2013)) fundamentally changed the enforcement situation: instead of protecting a one-time purchase, Adobe now validates subscriptions continuously through cloud authentication. This "always-connected" model provides a built-in enforcement mechanism that streaming services lack: while Netflix must verify location during playback, Adobe verifies identity and license validity during software launch, making the enforcement architecture fundamentally different.

However, a hybrid future appears to be emerging in the form of **"Always-Online DRM"**. Features like Adobe's cloud-dependent generative tools (Firefly, Neural Filters) require authenticated connections to function, effectively merging network-based verification with identity authentication. As more software features migrate from local computation to cloud processing, the distinction between "downloaded software" and "streamed content" blurs. Adobe's Fortress Index of 5.48% may therefore understate its future enforcement trajectory: as cloud-dependent features become the primary value proposition, Adobe may converge toward the Content Fortress model, where the delivery mechanism itself enforces geographic restrictions. This convergence raises important questions about the impact of such mechanisms on user privacy and security (Lindsay & Ricketson, 2006). This reflects the "Opportunities and Risks" of SaaS adoption (Benlian & Hess, 2011), where control shifts from the client device to the cloud provider.

The Utility Paradox thus reveals a broader pattern in digital economics: the enforcement mechanism available to a firm depends not on its pricing strategy

or market power, but on the *technical architecture of value delivery*. Downloaded software can embed cryptographic verification, streamed content requires network-level control, and ecosystem-embedded services leverage identity dependencies. As these architectures converge through cloud computing and AI-dependent features, the strategic archetypes identified in this study may themselves evolve, potentially collapsing the current diversity of enforcement approaches into a more uniform "cloud fortress" model where all digital services require continuous authenticated connections. The accelerating integration of AI into digital services reinforces this trajectory: features such as Adobe's Firefly generative tools or Spotify's AI-curated playlists are inherently server-side, requiring real-time authentication that simultaneously enables geographic enforcement as a by-product of the service architecture itself.

5.1.5. The Adversarial Cycle: A View Over Time

The relationship between providers and consumers is not static. Our historical analysis reveals a clear "Action-Reaction" cycle, visualized in Figure 11.

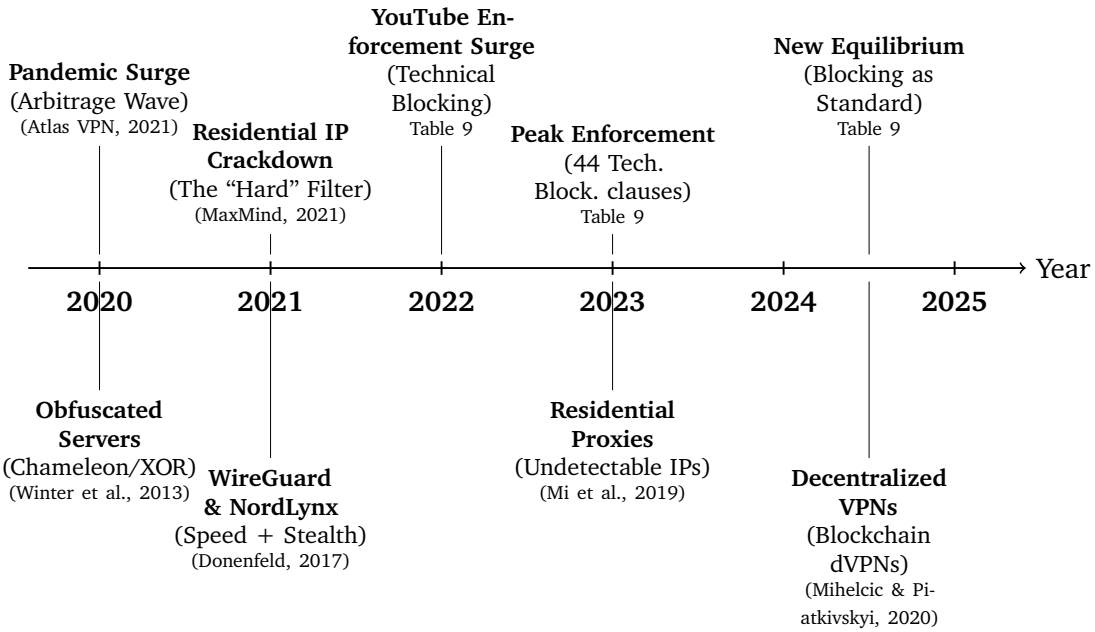

Figure 11.: The Adversarial Timeline: Coercive Barriers vs. Technical Circumvention (2020–2025). Events above the timeline reflect corporate enforcement measures documented in the ToS analysis; events below the timeline represent circumvention technologies.

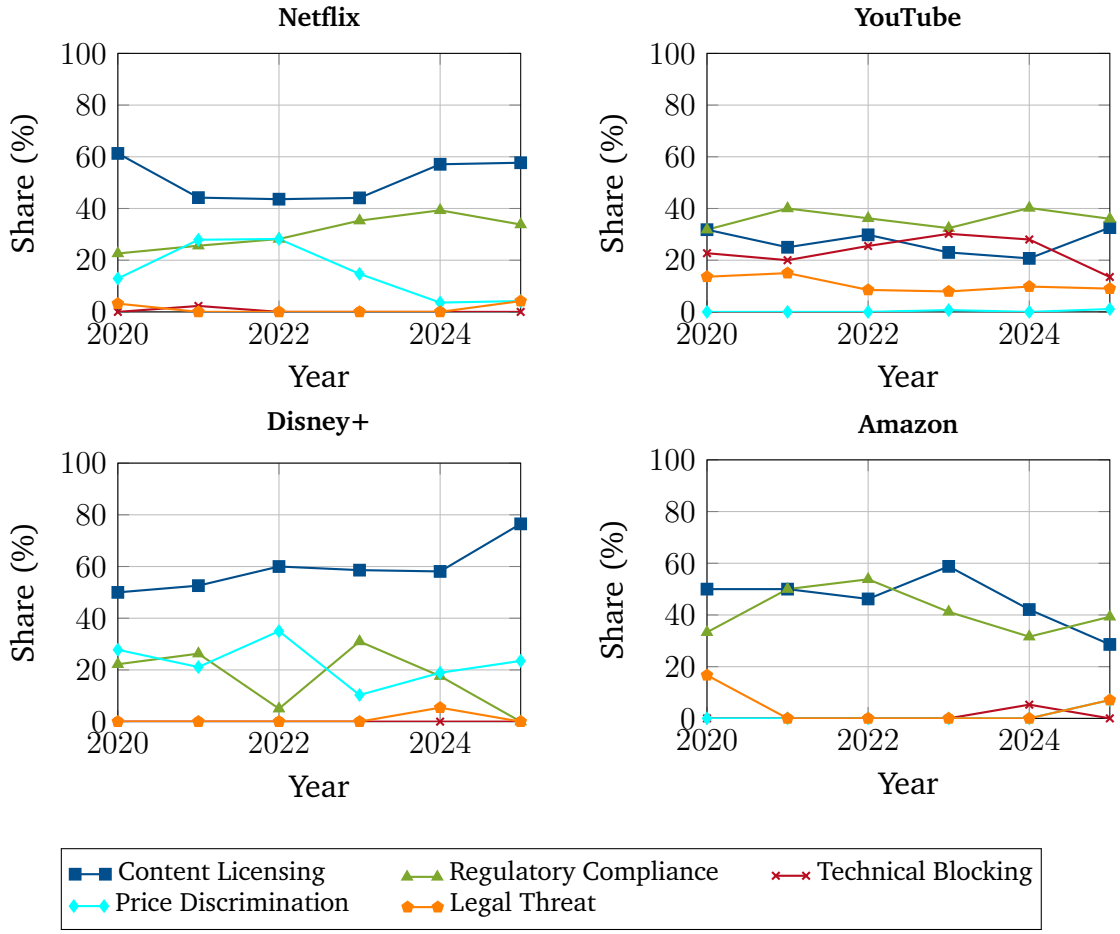

Figure 12.: Strategic Evolution: Video Streaming Leaders (2020–2025). Grouping Netflix, YouTube, Disney+, and Amazon Prime.

This timeline illustrates the dynamic relationship between corporate enforcement and consumer behavior. Early enforcement measures by streaming providers led VPN providers to develop “Obfuscated Servers” (techniques similar to those used to circumvent China’s Great Firewall (Ensafi et al., 2015)), which subsequently led to more sophisticated blocking techniques (circa 2021). This pattern suggests an ongoing adaptation process on both sides.

The adversarial cycle can be decomposed into four distinct phases, each characterized by a shift in the balance of power between platforms and circumvention tools:

Phase 1: The Wild West (Pre-2020). In the earliest phase of widespread streaming, geographic enforcement was minimal and inconsistent. Many platforms

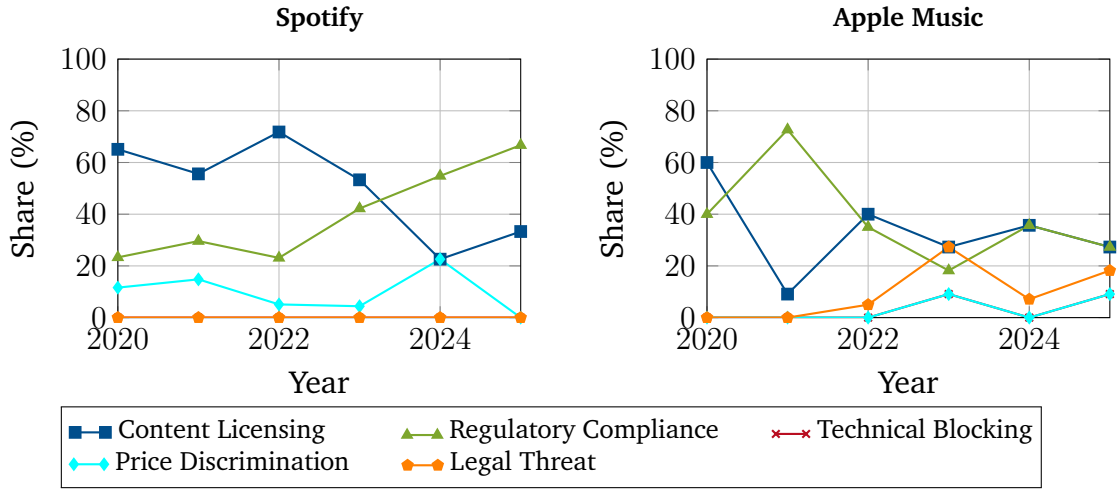

Figure 13.: Strategic Evolution: Music Streaming (2020–2025). Compared with the video streaming leaders in Figure 12, music services show markedly lower Technical Blocking intensity. Spotify shows zero Technical Blocking clauses across the entire period, while Apple Music shows only intermittent spikes.

relied solely on IP geolocation databases that were easily circumvented by any commercial VPN. During this period, geo-arbitrage was effectively risk-free, as platforms lacked both the technical infrastructure and the institutional motivation to actively police subscriber locations. Netflix's initial global expansion in January 2016 (Netflix, 2016) and the subsequent splitting of the streaming market into competing services created the conditions for widespread arbitrage by multiplying both the number of services and the aggregate savings available to circumventing users.

Phase 2: The First Wall (2020–2021). The COVID-19 pandemic dramatically accelerated VPN adoption as remote work normalized the use of virtual networking tools (Atlas VPN, 2021). Simultaneously, streaming subscriptions surged globally, everyone was stuck at home, increasing the economic stakes of geo-arbitrage for platforms. In response, services began deploying dedicated IP blacklisting infrastructure, partnering with specialized geolocation companies to identify and block known VPN exit nodes (MaxMind, 2021). This period corresponds to the "Residential IP Crackdown" noted in our timeline (Figure 11), where platforms shifted from blocking known datacenter IP ranges to attempting to identify residential proxy services.

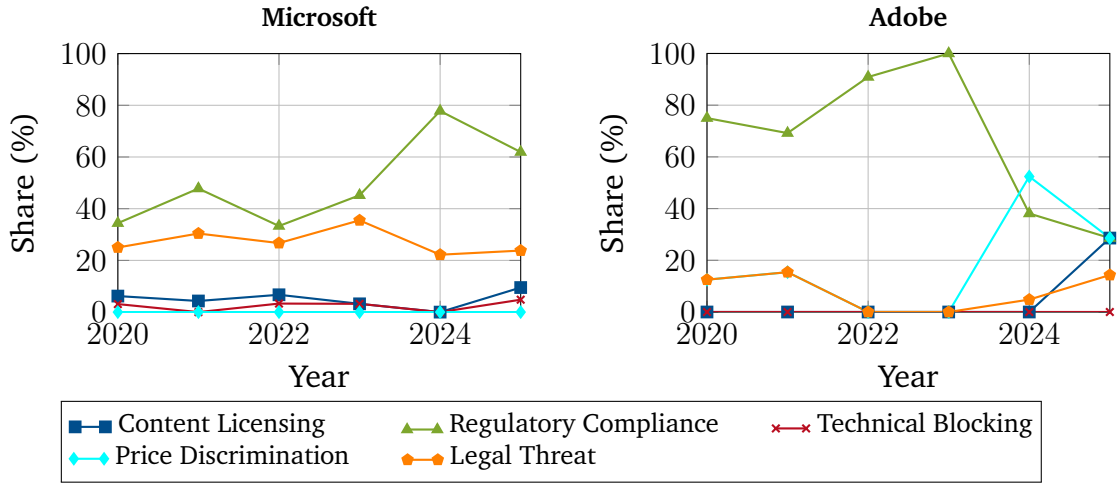

Figure 14.: Strategic Evolution: Software Utilities (2020–2025). Microsoft and Adobe show distinct patterns from streaming services, relying more on Regulatory Compliance and Legal Threats than Technical Blocking.

Phase 3: The Escalation (2022–2023). Our data shows a dramatic turning point in 2022–2023, driven primarily by YouTube's enforcement surge (Table 6: from 16 incidents in 2022 to 53 in 2023). This phase is characterized by the deployment of multi-signal detection: platforms moved beyond simple IP-based blocking to incorporate billing address verification, payment method geolocation, and behavioral analytics. The shift from passive to active enforcement is clearly visible in the ToS language, which evolved from permissive constructions ("We may restrict access...") to prohibitive directives ("You must not use any technology to disguise your location"). This linguistic shift, documented in our tone analysis (Section 3.3.2), reflects a strategic decision to make the consequences of circumvention explicit and unmistakable.

Phase 4: The New Equilibrium (2024–Present). The most recent phase shows a partial stabilization, with Technical Blocking counts declining from their 2023 peak (44 to 24 in 2024, Table 9). This does not necessarily indicate relaxed enforcement. Rather, it likely reflects the integration of blocking measures into standard operational procedures. Once a firm has established its detection infrastructure and updated its ToS, the need for *new* enforcement clauses diminishes. The blocking technology becomes part of the background architecture rather than a point of active policy development. Meanwhile, VPN providers have responded with increasingly sophisticated obfuscation technologies, including traffic shap-

ing that mimics regular HTTPS patterns, distributed residential exit nodes, and protocol-level stealth features (Winter et al., 2013). Beyond simple IP masking, a new generation of VPN products now aims to provide consumers with complete anonymous digital identities, bundling region-specific payment methods, temporary email addresses, and browser fingerprint randomization into integrated toolkits. Decentralized VPN architectures (Mihelcic & Piatkivskyi, 2020) further complicate platform enforcement by routing traffic through peer-to-peer networks of residential nodes rather than identifiable commercial server infrastructure. The result is an uneasy equilibrium where both sides have invested heavily in competing technologies, and the marginal cost of gaining a further advantage is rising for both platforms and circumvention providers.

5.2. The Secret Tech Race

Returning to the history of piracy, the modern world is defined by a growing tech race. Our research shows that companies are getting much better at finding where users really are, even with a high-quality VPN. They no longer just block IP addresses. They use advanced tools like Deep Packet Inspection (Deep Packet Inspection (DPI)), AI to read traffic fingerprints, and browser fingerprinting techniques (Laperdrix et al., 2020). Machine learning approaches to VPN traffic classification have become increasingly sophisticated (Dainotti et al., 2012), enabling platforms to detect circumvention attempts even when traditional IP-based blocking fails.

Based on the available technical literature and our document analysis, the technical escalation can be conceptualized as a multi-layered detection stack. At the first layer, platforms maintain databases of known VPN and proxy IP addresses (MaxMind, 2021), blocking connections from these ranges. This is the simplest form of detection but also the easiest to circumvent, as VPN providers regularly rotate their IP addresses. At the second layer, platforms analyze traffic patterns, as VPN connections often exhibit distinctive packet sizes, timing patterns, and protocol signatures that differ from regular browsing traffic, even when encrypted. At the third layer, platforms employ browser and device fingerprinting to detect

inconsistencies: a user whose browser reports a German timezone and language setting but connects from a Turkish IP address raises a detection flag. At the most advanced layer, some platforms reportedly use behavioral analytics, tracking usage patterns (login times, content preferences, payment history) to identify accounts that are likely being used from a different region than their registered location.

On the circumvention side, VPN providers have responded with equally sophisticated countermeasures. Obfuscated server protocols (such as NordVPN's "NordLynx" or Surfshark's "Camouflage Mode") disguise VPN traffic to look like regular HTTPS browsing. Residential proxy services route traffic through real home internet connections, making it indistinguishable from genuine local traffic. Some services even offer dedicated IP addresses that are not shared with other users, reducing the likelihood of blacklisting.

However, a key challenge for research is that these tools are kept secret. Unlike the open legal fights over Napster, modern geo-blocking happens in private. Companies keep their methods secret so that VPN providers can't adapt. This means that while we can see an increase in blocking, it is hard to say exactly how the technology works. This opacity creates a significant methodological challenge: the most important enforcement mechanisms are precisely those that are least observable to researchers. Our ToS analysis captures the *stated* enforcement approach, but the *actual* technical capabilities may be significantly more advanced than what firms publicly disclose.

5.3. Aggregate Enforcement Trends

This section provides a deeper look at the data, analyzing the specific numbers that drive the strategic trends.

To understand the macro-trends, we analyze how the total volume of policy text has shifted. Our analysis shows the overwhelming dominance of General Terms (legal boilerplate), which consistently make up over 90% of all sentences (see Table 9). However, when we filter for *strategic* categories (Figure 15), a clear pattern emerges: **Content Licensing** and **Regulatory Compliance** are the baseline "noise"

of digital business, while **Technical Blocking** and **Account Action** show specific, event-driven spikes.

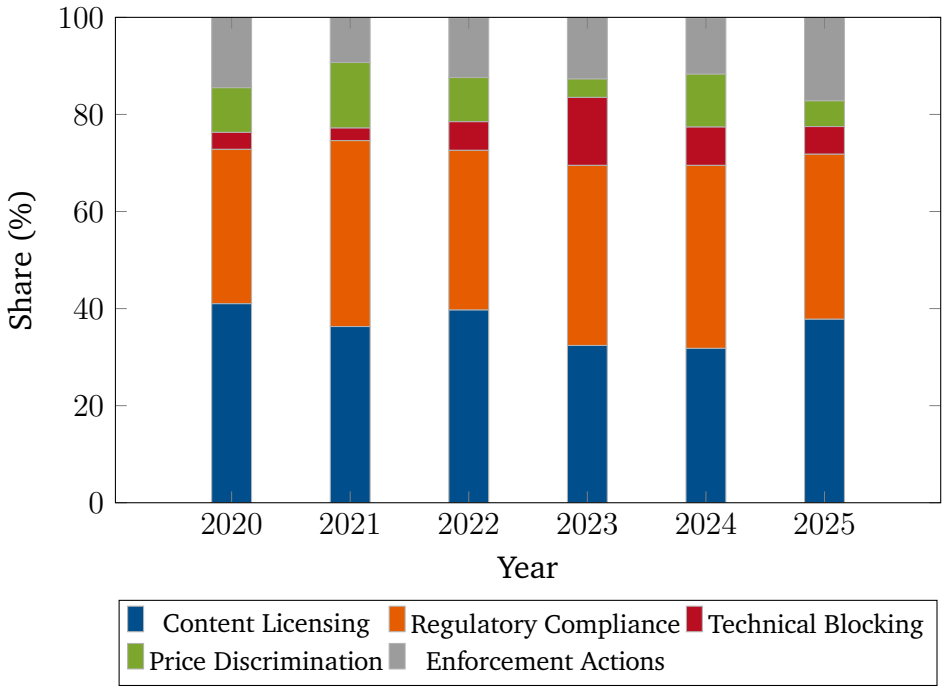

Figure 15.: Distribution of Policy Text Categories Over Time (Strategic Categories Only).

As illustrated in the preceding analysis, the strategic categories are overwhelmingly overshadowed by general terms, which constitute over 90% of all sentences (Table 9). Consequently, the strategic trends are best visualized by focusing exclusively on non-boilerplate categories, as shown in Figure 15.

5.3.1. Service-Level Enforcement Trends

At the service level (Table 6), two patterns stand out. Microsoft maintains a consistent low-level "background radiation" of legal checks without sudden spikes, consistent with the Enterprise Fortress archetype. YouTube's enforcement surge peaked in 2023 before declining in 2024–2025, suggesting a "cooldown" period where blocking rules became standard practice (see Section 4.3 for the full year-by-year breakdown).

5.4. Implications for Policy and Practice

The findings have important implications for several groups in the digital economy: platform operators, regulators, VPN providers, and consumers.

5.4.1. Implications for Platform Operators

The strategic archetypes identified in this thesis suggest that firms should align their enforcement strategy with their underlying value delivery architecture rather than pursuing a "one-size-fits-all" approach to geo-arbitrage.

Content streaming platforms (Netflix, YouTube, Disney+) should consider whether the escalating costs of the "Content Fortress" approach (both in terms of technology investment and user friction) justify the revenue protection achieved. Netflix's strategic pivot toward global original content production represents a potentially more sustainable long-term response than ever-more-sophisticated blocking technology. By owning content globally, platforms eliminate the territorial licensing constraints that necessitate geo-blocking in the first place, effectively making the "fortress" unnecessary.

Software providers (Adobe, Microsoft) already benefit from identity-based enforcement that is more robust than network-based blocking. These firms should focus on strengthening subscription management and license validation rather than investing in VPN detection technologies that are more relevant to streaming platforms. The migration toward cloud-dependent features (e.g., Adobe Firefly) naturally strengthens enforcement without requiring explicit anti-circumvention measures.

Ecosystem platforms (Apple, Amazon) should recognize that their multi-service bundle strategy provides the most durable form of protection against geo-arbitrage. The switching costs embedded in ecosystem dependencies create natural barriers that are far more difficult to circumvent than any technical blocking system. Strategic investments in deepening ecosystem integration (e.g., linking subscription

pricing to hardware ownership or loyalty programs) may be more effective than direct enforcement.

5.4.2. Implications for Regulators

The Affordability Paradox documented in this study highlights a tension that regulators should address. On one hand, geographic price discrimination enables digital inclusion by making services affordable in lower-income markets. On the other hand, the enforcement measures required to maintain this discrimination impose costs on legitimate users (travelers, expatriates, students abroad) and raise questions about digital sovereignty and consumer rights.

The EU's Geo-Blocking Regulation (2018/302) represents one approach, prohibiting unjustified geo-blocking within the single market (European Union, 2018). As Trimble (2024) comprehensively documents, this regulation exempts audiovisual content, precisely the category where our data shows the highest enforcement intensity. Regulators should consider whether this exemption remains justified as content licensing models evolve and as the social costs of aggressive enforcement (false positives, privacy intrusions through behavioral analytics, restricted portability) become more apparent. Zuiderveen Borgesius and Poort (2017) argue that geographic price discrimination in digital markets raises significant data privacy concerns under EU law, as the detection technologies required to enforce regional pricing, including IP geolocation, behavioral tracking, and payment verification, necessarily involve processing personal data.

Our finding that firms with more harmonized global pricing require less enforcement spending suggests a potential "regulatory nudge" approach (Thaler & Sunstein, 2003): rather than prohibiting geo-blocking directly, regulators could incentivize price harmonization through transparency requirements (mandating disclosure of regional price differences) or through competition policy measures that address the territorial licensing practices underlying content division (Gomez-Herrera et al., 2016).

5.4.3. Implications for Consumers

The Three-Level Mechanism analysis (Section 2.2) reveals that consumers often underestimate the broader consequences of geo-arbitrage. While individual acts of price hopping may seem victimless, our analysis suggests three systemic risks.

First, if geo-arbitrage becomes widespread enough to significantly erode revenue from low-price markets, firms may respond by raising prices in those markets, harming the local consumers the pricing was designed to serve. There is already evidence of this dynamic: YouTube's enforcement surge in 2023, documented in our ToS analysis (Table 9), coincided with reported price increases in markets such as Turkey and Argentina. While our DSPI captures only a December 2025 snapshot and does not include longitudinal price data, this overlap in timing suggests that platforms may raise prices in "exploited" markets partly in response to arbitrage losses. This creates a harmful outcome where the consumers least able to afford price increases bear the costs of circumvention behavior by wealthier users in other countries.

Second, the enforcement technologies deployed to combat arbitrage (behavioral analytics, device fingerprinting, payment verification) create surveillance infrastructure that extends well beyond its original purpose, with implications for digital privacy that affect all users, not just those engaging in circumvention. As Zuiderveen Borgesius and Poort (2017) argue, the data collection required to enforce geographic pricing, including IP tracking, payment method analysis, and behavioral profiling, raises significant concerns under data protection frameworks such as the EU's General Data Protection Regulation (General Data Protection Regulation (GDPR)). The irony is that privacy-enhancing technologies (VPNs) used for arbitrage are met with privacy-reducing technologies (fingerprinting, behavioral analytics) deployed for enforcement, creating an escalating cycle that erodes digital privacy for all users.

Third, consumers who engage in geo-arbitrage face tangible individual risks that are often downplayed in online communities. Account termination without refund, loss of accumulated content libraries (e.g., purchased films, saved playlists, cloud-stored files), and potential legal liability in jurisdictions where ToS violations carry contractual penalties represent real costs that may only materialize months

or years after the initial arbitrage decision. While online communities such as Reddit do share enforcement experiences alongside success stories, the information environment remains skewed: successful circumvention is an ongoing, visible state (the subscription continues to work), whereas enforcement actions are discrete, often embarrassing events that users may attribute to unrelated causes or simply move on from without detailed reporting. This structural asymmetry, compounded by the self-selecting nature of active forum participants, means that the *perceived* probability of detection in these communities likely understates the actual enforcement rate.

5.5. Limits of the study

While this study gives us a new way to look at geo-arbitrage, there are some limits to our findings.

5.5.1. Sample Size and Generalizability

The correlation analysis relies on a strategic sample of $N = 10$ digital service providers. While these firms represent a significant majority of the consumer subscription market by revenue and user base, the sample is small in statistical terms. With 10 observations, correlation coefficients are inherently unstable: a single outlier can substantially shift the Pearson r value, as demonstrated by the dramatic reversal from $r = -0.55$ (full sample) to $r = +0.35$ (excluding VPN providers), not merely a reduction in size but a complete sign change driven by the removal of just two data points. Consequently, the findings should be interpreted as "exploratory" evidence of strategic archetypes rather than a definitive "law" of digital economics.

The country sample ($N = 11$) presents a similar limitation. While the purposive layered sampling strategy ensures representation across income levels and geographic regions, the exclusion of major markets such as India (the world's second-largest internet market by user base), China (where VPN usage is subject to state-level regulation), and several African economies limits the generalizability

of the DSPI findings. These markets may exhibit pricing patterns and enforcement dynamics that differ substantially from those observed in our sample, particularly given the unique regulatory environments in China and the rapidly growing digital economies of Sub-Saharan Africa.

Future research could expand this dataset to include mid-tier SaaS providers, gaming platforms (e.g., PlayStation Plus, Nintendo Online), and emerging AI subscription services (e.g., ChatGPT Plus, Midjourney) to test whether the "Enterprise Fortress" model holds for smaller B2B firms and whether new service categories develop their own distinct strategic archetypes.

5.5.2. The "Average Citizen" Bias (Socioeconomic Mismatch)

Our "Affordability" metric calculates cost as a percentage of the *Median National Monthly Wage*. However, in emerging markets like Turkey or Argentina, the target demographic for services like Netflix or Adobe is likely the urban upper-middle class, whose income is significantly higher than the national average.

For instance, World Bank data indicate that in Turkey, the top 20% of earners capture nearly 48% of total disposable income (World Bank, 2023). Similarly, in Argentina, the top 10% of earners have average monthly incomes exceeding $496 USD, well above the national median (INDEC, 2023). This implies that global digital services are aggressively priced to target this specific "Global Elite" segment. As Kastanakis and Balabanis (2012) argue, in markets with high income inequality, luxury consumption (including premium digital subscriptions) serves as a critical status signal for the upper class. This "Elite Targeting" pricing strategy explains why firms tolerate some level of piracy from the lower 80%—they were never the primary customer segment to begin with.

The Digital Services Price Index (DSPI) represents a snapshot of pricing data from December 2025. In hyperinflationary economies such as Argentina and Turkey (both classified as hyperinflationary under IAS 29 (IFRS Foundation, 2023)), local currency prices are adjusted frequently in response to macroeconomic conditions. A "cheap" arbitrage opportunity identified in this thesis could be eliminated by a

price adjustment or currency devaluation. The "Arbitrage Window" is therefore dynamic rather than static.

5.5.3. AI Classification Reliability

The use of LLMs (Gemini 3 Flash) creates a potential "Black Box" validity risk. To reduce this, we used the model's self-reported confidence scores as a filtering mechanism. The final dataset achieved an average confidence score of **0.947**, with **80.5%** of classifications exceeding a confidence threshold of 0.9. This high degree of certainty suggests that the detection of "coercive" vs. "general" language is reliable, even without human verification for every datapoint.

5.5.4. Document-Based Analysis Limitations

A fundamental limitation of this study is its reliance on publicly available documents (ToS, annual reports, earnings calls) as proxies for corporate strategy. The assumption that stated policy reflects actual enforcement behavior is not perfect. Companies might use strict rules for legal safety but only enforce some of them, or they may employ undisclosed detection technologies that extend beyond the scope of their stated policies. The "Secret Tech Race" discussed in Section 5.2 highlights this gap: the most effective enforcement technologies are precisely those that firms have the strongest motivation to conceal. Future research could complement document-based analysis with experimental methods (e.g., systematically testing VPN access across services and regions) to measure actual enforcement rates rather than stated policies.

The forward-fill strategy (Chapter 3), which added 700 carry-forward observations (2.8% of the time-series dataset), assumes that policies remain unchanged between documented updates. While this is reasonable because ToS typically remain legally active until explicitly revised, it may overcount the persistence of specific clauses if internal policies change without a formal document update.

5.5.5. Methodological Reflections

Beyond the substantive findings, this study shows important methodological lessons for researchers working with corporate legal documents. As documented in Section 3.3.2, the Gemini 3 Flash model dramatically outperformed the traditional BERT-based Zero-Shot classifier (26.8% agreement, Cohen's Kappa $= 0.032$), confirming that advanced generative models are essential for legal text analysis where the task requires distinguishing between the mere *mention* of a concept and its active *regulation*, a distinction that keyword-sensitive NLI models cannot reliably make. This is consistent with Gilardi et al. (2023), who demonstrated that large language models outperform traditional approaches in complex text annotation tasks.

This finding suggests that future research on complex legal texts should employ advanced generative models rather than traditional NLI approaches, particularly when the classification task requires distinguishing between the mere *mention* of a concept and its active *regulation*. However, the use of LLM-based classification introduces its own reproducibility challenges. Model outputs can vary between API versions, and the specific weights and training data of Gemini 3 Flash may not be available for future replication. To mitigate this, we have documented the exact system prompt (Listing 3.1), batch processing parameters, and confidence thresholds used in our pipeline, enabling methodological reproducibility even if exact numerical reproduction is not guaranteed. The complete source code, data processing pipelines, and the master dataset are publicly available in the accompanying GitHub repository (Weckbach, 2025). We recommend that future studies employing LLM-based classification adopt a similar transparency protocol: publishing the complete system prompt, documenting the model version and API parameters, and reporting confidence score distributions alongside classification results.

6. Conclusion

This chapter sums up the findings, discusses what the study adds to the literature, and notes its limitations. Finally, we look at how new regulations and technologies may keep changing the digital services market.

6.1. Summary of Key Findings

This thesis examined the strategic conflict between firms' price discrimination practices and consumer-driven geo-arbitrage in digital subscription markets. The study combined a novel quantitative index (the DSPI) with LLM-based qualitative analysis of corporate documents to provide the first complete mapping of both the economic forces driving geo-arbitrage and the strategic responses firms deploy to counter it.

Regarding **RQ1 (Economic Incentive)**, the DSPI reveals substantial and systematic price differences across markets. The analysis of up to 11 digital services across 11 countries demonstrates that subscriptions in low-income markets can cost up to 90% less than identical services in high-income markets (e.g., YouTube Premium in Pakistan at 12% of the US price, Spotify in Pakistan at 10% of the US price). These differences are not arbitrary. They follow a broadly predictable pattern aligned with national income levels, consistent with third-degree price discrimination theory (Varian, 1989). However, the complementary PTW analysis reveals an **Affordability Paradox**: these nominally "cheap" prices are often significantly more expensive for local consumers in real terms (Section 4.2), fundamentally challenging the popular narrative that low-income markets receive "bargain" prices and reframing the arbitrage motivation as an exploitation of welfare-enhancing pricing structures.

Regarding **RQ2 (Strategic Response)**, enforcement strategies are primarily determined by **Business Model Architecture** rather than by the extent of price

differences. This is the study's most surprising finding. Content streaming firms enforce strict geographic blocking due to licensing requirements, with YouTube exhibiting the highest Fortress Index (33.68%) among content providers. Software firms like Microsoft rely on identity verification and legal threats rather than network-based blocking, reflecting the "Enterprise Fortress" archetype. Ecosystem platforms (Apple, Amazon) leverage multi-service bundle dependencies as implicit enforcement, making arbitrage impractical without relocating one's entire digital identity. VPN providers, by their nature, implement no geographic restrictions, instead framing circumvention as a privacy right.

Beyond the two research questions, the **enforcement evolution** analysis reveals a clear escalation in enforcement intensity, peaking in 2023 before stabilizing (Table 9). This surge, driven primarily by YouTube's enforcement campaign, coincides with post-pandemic increases in VPN adoption and geo-arbitrage awareness. The subsequent stabilization suggests that firms have moved from active enforcement expansion to maintenance of established blocking infrastructure. However, the constant presence of circumvention discussions in online communities suggests these barriers increase friction rather than eliminating arbitrage entirely, consistent with the game-theoretic prediction (Equation 2.1) that perfect enforcement is neither achievable nor economically optimal.

Taken together, these findings paint a picture of a digital economy in transition. The current regime of territorial price discrimination, inherited from the pre-digital era of physical media distribution and broadcast licensing (Lobato, 2019), is under growing pressure from the inherently borderless nature of digital delivery. Firms' responses to this pressure, whether through technological fortress-building, ecosystem lock-in, or adaptive global pricing, reveal fundamentally different theories about how digital markets should function. The long-term trajectory, informed by the piracy parallel developed in Chapter 2, suggests that adaptive strategies (reducing the arbitrage motivation through pricing innovation) may prove more sustainable than coercive strategies (raising the cost of circumvention through technology).

6.2. Contribution to Research

This study adds both methods and theory to digital economics.

6.2.1. Methodological Contributions

The Digital Subscription Price Index

The DSPI was created as a new way to measure price discrimination for digital services. Unlike existing price indices (such as the Big Mac Index or the iPod Index), which measure a single product, the DSPI captures a basket of digital services across multiple categories, providing a fuller picture of digital pricing patterns. The complementary PTW ratio adds an affordability dimension that purely nominal indices lack. Together, these metrics offer a replicable framework that future researchers can apply to track pricing changes over time or extend to additional service categories.

AI-Assisted Legal Analysis

This study demonstrates that generative LLM models can successfully analyze thousands of legal sentences with high reliability (average confidence 0.947), significantly outperforming traditional NLI models for complex legal text classification. The pipeline architecture (combining structured system prompts, batch processing, and forward-fill gap handling) provides a replicable template for future research on corporate policy documents at scale. This contribution is particularly relevant given the rapid growth of ToS documents, which makes traditional manual coding increasingly impractical.

6.2.2. Theoretical Contributions

Extension of Business Model Innovation Theory

The study extends BMI theory by showing that consumer bypassing behaviors work as a disruptive force similar to technological innovation, forcing firms to fundamentally change their value capture mechanisms. This finding adds a new category of external pressure to the BMI literature, which has traditionally focused on competitor-driven or technology-driven disruption (Foss & Saebi, 2017). Consumer-driven disruption through circumvention technology represents a distinct mechanism where the disruption originates from the demand side rather than the supply side.

Strategic Archetypes

The identification of four distinct types (Content Fortress, Ecosystem Fortress, Enterprise Fortress, Utility Paradox) provides a framework for understanding how different business models respond to the same external threat. The key finding that business model architecture is a stronger predictor of enforcement strategy than price gap size challenges the intuitive assumption that firms with the largest price differences would also have the strongest enforcement. Instead, the delivery mechanism (streaming vs. download vs. ecosystem) determines the available enforcement tools.

The Piracy-Arbitrage Parallel

By drawing explicit parallels between the digital piracy wave of the 2000s and modern geo-arbitrage, this thesis contributes to a longer-term understanding of how digital disruption forces business model adaptation. The historical comparison suggests that the current enforcement-heavy phase may eventually give way to adaptive strategies. This contribution is distinct from the existing piracy literature (Oberholzer-Gee & Strumpf, 2007; Peukert et al., 2017) because it identifies geo-arbitrage as a *qualitatively different* form of consumer circumvention (one

involving payment rather than theft, location rather than access) that nonetheless triggers similar strategic responses from firms. This suggests that the dynamics of disruption and adaptation in digital markets may follow recurring patterns regardless of the specific circumvention mechanism, a finding with implications for anticipating firm responses to future forms of consumer-driven boundary-crossing.

The Affordability Paradox

The documentation of the Affordability Paradox, that nominally "cheap" prices in low-income markets are often more expensive in real terms (relative to local wages) than high-income market prices, challenges a widespread assumption in both the popular press and the academic literature that price discrimination in digital markets primarily benefits consumers in developing economies. By demonstrating that a Netflix subscription in Argentina consumes over twelve times the share of monthly income compared to the USA, this finding reframes the equity debate around geo-arbitrage and provides empirical grounding for policy discussions about digital inclusion and fair pricing.

6.3. The Future

Geo-blocking is expected to undergo significant changes in the coming years.

6.3.1. Regulatory Evolution

As rules like the EU's Digital Single Market evolve (building on regulations such as the EU Geo-Blocking Regulation (European Union, 2018)), geo-blocking practices may change significantly. The current regulation exempts audiovisual content from its prohibition on unjustified geo-blocking, but this exemption is subject to periodic review, and the European Commission has signaled interest in expanding the regulation's scope (Trimble, 2024). New laws might move companies away from blocking and toward keeping prices the same everywhere. Gomez-Herrera et al. (2016) provide evidence that geo-blocking within the EU reduces consumer welfare

and digital market integration. Beyond the EU, emerging digital trade agreements (such as the Digital Economy Partnership Agreement between Singapore, Chile, and New Zealand) may establish new norms around cross-border digital access that put additional pressure on territorial pricing models. The tension between national tax regimes (which incentivize location-based pricing) and consumer expectations of borderless digital access will likely intensify as digital services become a larger share of household expenditure globally.

6.3.2. Technological Evolution

The arms race between blocking technology and bypassing tools shows no signs of slowing. Advanced techniques such as residential IP proxies, browser fingerprinting, and machine learning-based detection create a technically complex environment that demands continuous investment from both sides. On the enforcement side, the integration of artificial intelligence into detection systems, including behavioral pattern recognition and cross-signal analysis, promises to make VPN detection more accurate but also more invasive. On the circumvention side, emerging technologies such as decentralized VPN networks (Decentralized Virtual Private Networks (dVPNs)) built on blockchain infrastructure (Mihelcic & Piatkivskyi, 2020) could make traditional IP-based blocking fundamentally ineffective by distributing exit nodes across millions of individual devices rather than identifiable data centers. Researchers should investigate whether the rising cost of this arms race eventually makes geographic price discrimination economically unsustainable, particularly for smaller platforms that cannot afford enterprise-grade detection infrastructure.

6.3.3. Market Convergence

Ultimately, the cycle of blocking and bypassing may end not through better technology, but through market forces that promote global price convergence (Goldfarb & Tucker, 2019). As digital services become increasingly standardized and competition intensifies, companies may find that the costs of maintaining differentiated regional pricing, including enforcement technology, legal compliance, user friction,

and reputational damage, outweigh the incremental revenue gained from price discrimination (Varian, 1989). The music industry's trajectory offers a precedent: Spotify's pricing has converged significantly across markets compared to the highly fragmented pricing of the iTunes store era (Aguiar & Waldfogel, 2018a; Waldfogel, 2010), suggesting that mature digital markets trend toward simpler, more uniform pricing structures. In such a scenario, geo-arbitrage would become obsolete, not because users are blocked, but because there is no longer a meaningful price difference to exploit. However, this convergence scenario assumes that income inequality between countries will narrow or that firms will accept lower margins in wealthy markets, assumptions that current macroeconomic trends do not uniformly support (Rogoff, 1996; World Bank, 2023).

6.3.4. Future Research

Future studies could build on this work in several directions. First, expanding the service sample beyond 11 services to include mid-tier SaaS providers, gaming platforms (e.g., PlayStation Plus and Steam), and emerging categories (e.g., AI subscription services like ChatGPT Plus or Midjourney) would test whether the strategic archetypes identified here generalize across the broader digital economy. Second, longitudinal tracking of the DSPI over multiple years would capture how companies adjust prices in response to macroeconomic events (currency devaluations, inflation spikes) and regulatory changes, transforming the current snapshot into a dynamic monitoring tool. Third, demand-side research using surveys or interviews with consumers who engage in geo-arbitrage would complement this supply-side analysis, particularly regarding ethical perceptions, risk assessment, and the social dynamics of circumvention communities. Fourth, comparative regulatory analysis across jurisdictions (e.g., the EU's Geo-Blocking Regulation versus the absence of equivalent legislation in North America or Asia) would help isolate the causal effect of legal frameworks on firm enforcement strategies. Finally, the methodological approach of LLM-based policy analysis could be extended to other domains where firms manage digital boundaries, such as data localization requirements, content moderation policies, or algorithmic pricing disclosures.

A. Detailed Service Evolution

This appendix presents evolution data for VPN providers (Figure 16), as the detailed evolution charts for other services have been integrated into Chapter 4 and Chapter 5.

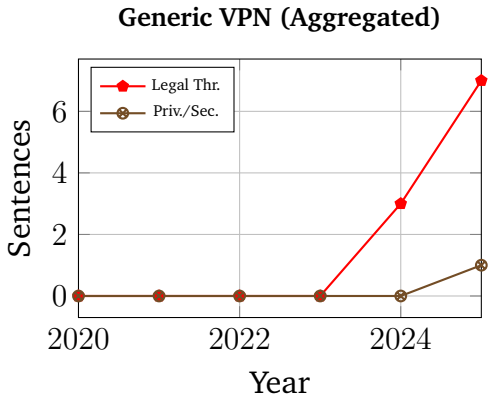

Figure 16.: Evolution of VPN Provider Enforcement. Note: Specific VPN graphs have been excluded for brevity as they show minimal variation.

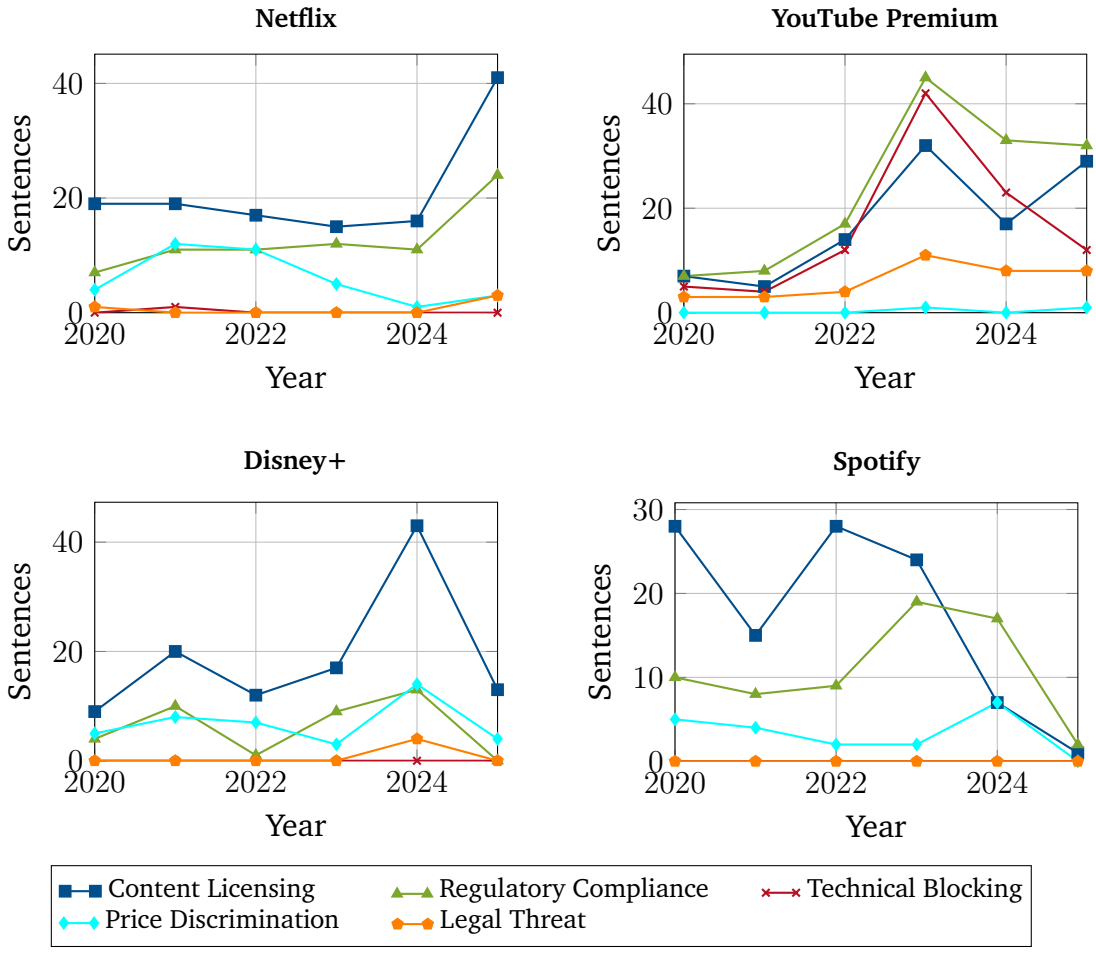

Figure 17.: Absolute Sentence Counts: Video and Music Streaming (2020–2025). Unlike the proportional charts in Chapter 5, this figure shows raw sentence counts to illustrate the volume of enforcement language.

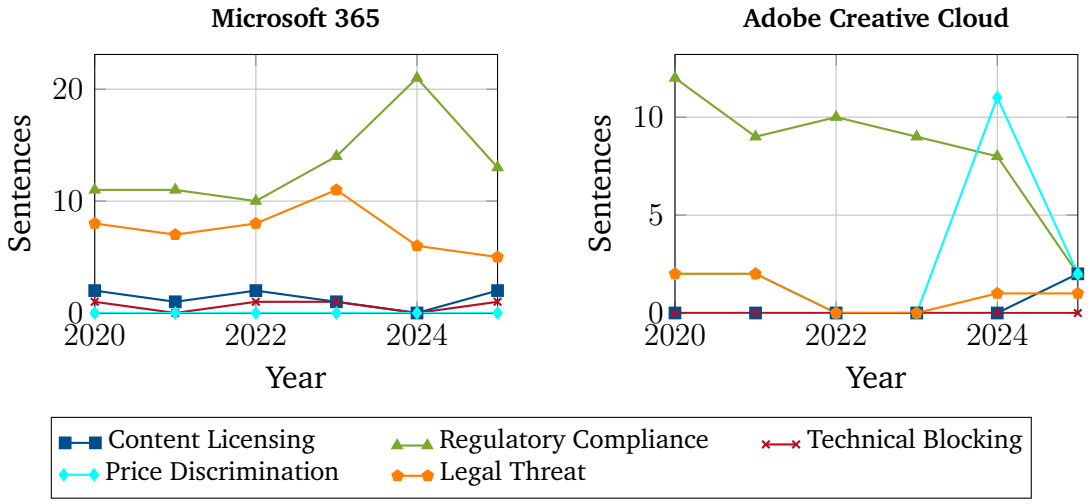

Figure 18.: Absolute Sentence Counts: Software Utilities (2020–2025).

B. Quantitative Reference Data

Table 10 documents the median monthly wage figures and exchange rates used to compute the DSPI and PTW metrics throughout this thesis. All exchange rates reflect market rates recorded in December 2025 at the time of data collection. The DSPI is calculated purely as the ratio of the USD-converted local price to the US baseline price (DSPI $=$ $\text{Price}_{\text{USD}}$ / US Baseline Price), without any wage adjustment. The PTW ratio is calculated separately as the subscription price expressed as a percentage of the median monthly wage (PTW $=$ $\text{Price}_{\text{USD}}$ / $\text{Monthly Wage}_{\text{USD}}$).

Table 10.: Median Monthly Wages and Exchange Rates Used for PTW Calculations (December 2025). Countries are ordered by USD wage (descending).

Country	Cur.	Monthly Wage	Rate to USD	Wage (USD)	Source
Switzerland	CHF	6,903	1.1300	7,800	(Swiss Federal Statistical Office, 2023)
United States	USD	6,600	1.0000	6,600	(OECD, 2023)
United Kingdom	GBP	4,500	1.2700	5,715	(OECD, 2023)
Germany	EUR	4,800	1.0900	5,232	(OECD, 2023)
Poland	PLN	6,700	0.2500	1,675	(Główny Urząd Statystyczny (GUS), 2024)[a]
Turkey	TRY	23,789	0.0320	761	(Turkish Statistical Institute, 2023)
Brazil	BRL	3,000	0.2000	600	(OECD, 2023)
Argentina	ARS	456,813	0.0012	548	(INDEC, 2023)
Ukraine	UAH	19,600	0.0260	510	(State Statistics Service of Ukraine, 2024)[a]
Philippines	PHP	20,583	0.0180	370	(Philippine Statistics Authority (PSA), 2024)[a]
Pakistan	PKR	70,700	0.0036	255	(Pakistan Bureau of Statistics (PBS), 2024)[a]

[a] Median estimate derived from national statistical office data (2024).

Table 11 presents the complete PTW matrix, showing the cost of each digital service as a percentage of the median monthly wage in each country. This table complements the nominal USD prices (Table 5) and the DSPI indices (Table 4) by expressing prices in affordability terms. Values above 10% indicate that a single subscription would consume more than a tenth of the median monthly income, highlighting the severity of the Affordability Paradox in low-income markets.

Table 11.: Complete PTW Matrix: Subscription Cost as % of Median Monthly Wage by Service and Country (December 2025). Cells marked "–" indicate the service is unavailable in that country. Values $\geq 10\%$ are highlighted in **bold**.

Country	*Netflix*	*YouTube*	*Disney+*	*Amazon*	*Spotify*	*Apple M.*	*MS 365*	*Adobe CC*	*Xbox GP*	*NordVPN*	*ExpressVPN*
Switzerland	0.33	0.26	0.24	0.14	0.23	0.20	1.45	1.11	0.14	1.35	1.35
United Kingdom	0.24	0.29	0.24	0.20	0.27	0.24	1.89	1.48	0.16	1.64	1.86
Germany	0.29	0.27	0.23	0.19	0.27	0.23	2.06	1.62	0.19	2.00	2.08
United States	0.27	0.21	0.20	0.23	0.18	0.17	1.51	1.06	0.15	1.46	1.61
Poland	0.73	0.58	0.52	0.16	0.36	0.33	6.42	5.25	0.55	4.90	7.18
Argentina	3.28	1.88	2.69	1.74	0.72	1.31	8.15	**12.93**	1.97	7.77	**17.83**
Turkey	1.22	0.32	1.89	0.29	0.42	0.25	**13.88**	6.84	1.13	**12.73**	**15.41**
Ukraine	1.60	0.50	–	1.49	0.98	0.98	**13.76**	8.00	1.48	**19.00**	**22.99**
Brazil	1.50	0.83	1.56	0.66	0.80	0.73	**16.97**	7.13	1.46	7.11	**16.29**
Philippines	2.18	0.92	1.21	0.72	0.82	0.68	**23.83**	**18.49**	1.56	**23.35**	**26.41**
Pakistan	1.13	0.67	–	0.85	0.49	–	**32.47**	**27.45**	0.71	**30.48**	**30.66**

Bibliography

Adobe Inc. (2013). Adobe launches Creative Cloud [Adobe corporate announcement of the transition from perpetual licenses to Creative Cloud subscriptions].

Aguiar, L., & Martens, B. (2016). Digital music consumption on the internet: Evidence from clickstream data. *Information Economics and Policy*, *34*, 27–43.

Aguiar, L., & Waldfogel, J. (2018a). As streaming reaches flood stage, does it stimulate or depress music sales? *International Journal of Industrial Organization*, *57*, 278–307. https://doi.org/10.1016/j.ijindorg.2017.06.004

Aguiar, L., & Waldfogel, J. (2018b). Netflix: Global hegemon or facilitator of frictionless digital trade? *Journal of Cultural Economics*, *42*(3), 419–445. https://doi.org/10.1007/s10824-017-9315-z

Alaveras, G., Gomez-Herrera, E., & Martens, B. (2017). *Geo-blocking of non audiovisual digital media content in the EU digital single market* (tech. rep.). JRC Digital Economy Working Paper 2017-03. https://doi.org/10.2139/ssrn.2983793

Amit, R., & Zott, C. (2001). Value creation in e-business. *Strategic Management Journal*, *22*(6-7), 493–520.

Amit, R., & Zott, C. (2012). Creating value through business model innovation. *MIT Sloan Management Review*, *53*(Spring), 41–49.

Anson, J., Boffa, M., & Helble, M. (2019). Consumer arbitrage in cross-border e-commerce. *Review of International Economics*, *27*(4), 1234–1251. https://doi.org/10.1111/roie.12424

Ariyarathna, L. (2022). Circumvention of geo-blocking, technological protection measures, and streaming. In *Streaming and copyright law* (pp. 125–162). Routledge. https://doi.org/10.4324/9781032260938-5

Atlas VPN. (2021). VPN usage surged during the pandemic as remote work became the norm [Atlas VPN Research Report. Original URL discontinued after Nord Security acquisition (2024). Archived version available at: https:

//web.archive.org/web/20240104161642/https://atlasvpn.com/vpn-adoption-index].

Balassa, B. (1964). The purchasing-power parity doctrine: A reappraisal. *Journal of Political Economy*, *72*(6), 584–596.

Becker, G. S. (1968). Crime and punishment: An economic approach. *Journal of Political Economy*, *76*(2), 169–217.

Belleflamme, P., & Peitz, M. (2015). Digital piracy: Theory. In *The oxford handbook of the digital economy* (pp. 489–530). Oxford University Press.

Benlian, A., & Hess, T. (2011). Opportunities and risks of software-as-a-service: Findings from a survey of IT executives. *Decision Support Systems*, *52*(1), 232–246.

Beunza, D., & Stark, D. (2004). Tools of the trade: The socio-technology of arbitrage in a wall street trading room. *Industrial and Corporate Change*, *13*(2), 369–400.

Blum, B. S., & Goldfarb, A. (2006). Does the internet defy the law of gravity? *Journal of International Economics*, *70*(2), 384–405. https://doi.org/10.1016/j.jinteco.2005.10.002

Brouthers, K. D., Geisser, K. D., & Rothlauf, F. (2016). Explaining the internationalization of ibusiness firms. *Journal of International Business Studies*, *47*, 513–534.

Brynjolfsson, E., Collis, A., Diewert, W. E., Eggers, F., & Fox, K. J. (2019). *GDP-B: Accounting for the value of new and free goods in the digital economy* (NBER Working Paper No. w25695). National Bureau of Economic Research.

Burnham, T. A., Frels, J. K., & Mahajan, V. (2003). Consumer switching costs: A typology, antecedents, and consequences. *Journal of the Academy of Marketing Science*, *31*(2), 109–126. https://doi.org/10.1177/0092070302250897

Cardona, M., Duch-Brown, N., & Martens, B. (2015). *Consumer perceptions of (cross-border) eCommerce in the EU digital single market* (tech. rep.). JRC Digital Economy Working Paper 2015-15. https://doi.org/10.2139/ssrn.2668597

Carneiro-Diaz, V., Grille-Zallas, A., & Lage-Etchart, D. (2025). Automated legal analysis of rental contract clauses using large language models. *SoftwareX*, *31*, 102337.

Cassel, G. (1918). Abnormal deviations in international exchanges. *The Economic Journal*, *28*(112), 413–415.

Cavallo, A. (2017). Are online and offline prices similar? evidence from large multi-channel retailers. *American Economic Review*, *107*(1), 283–303.

Cavallo, A., & Rigobon, R. (2016). *The billion prices project: Using online prices for measurement and research* (NBER Working Paper No. w22111). National Bureau of Economic Research. https://doi.org/10.3386/w22111

Chen, J., & Sheng, J. (2026). The economics of password sharing. *Information Systems Research*. https://doi.org/10.1287/isre.2024.1313

Clemons, E. K., Hann, I.-H., & Hitt, L. M. (2002). Price dispersion and differentiation in online travel: An empirical investigation. *Management Science*, *48*(4), 534–549.

Creswell, J. W., & Plano Clark, V. L. (2017). *Designing and conducting mixed methods research* (3rd). Sage Publications.

Cusumano, M. A., Gawer, A., & Yoffie, D. B. (2019). *The business of platforms: Strategy in the age of digital competition, innovation, and power*. Harper Business.

Dainotti, A., Pescape, A., & Claffy, K. C. (2012). Issues and future directions in traffic classification. *IEEE Network*, *26*(1), 35–40.

Danaher, B., & Smith, M. D. (2014). Gone in 60 seconds: The impact of the megaupload shutdown on movie sales. *International Journal of Industrial Organization*, *33*, 1–8.

Danaher, B., Smith, M. D., Telang, R., & Chen, S. (2014). The effect of graduated response anti-piracy laws on music sales: Evidence from an event study in France. *Journal of Industrial Economics*, *62*(3), 541–553. https://doi.org/10.1111/joie.12056

Déjean, S. (2009). What can we learn from empirical studies about piracy? *CESifo Economic Studies*, *55*(2), 326–352.

Donenfeld, J. A. (2017). WireGuard: Next generation kernel network tunnel. *Proceedings of the Network and Distributed System Security Symposium (NDSS)*. https://doi.org/10.14722/ndss.2017.23160

Duch-Brown, N., & Martens, B. (2016). *The economic impact of removing geo-blocking restrictions in the EU digital single market* (tech. rep.). JRC Digital Economy Working Paper 2016-02. https://doi.org/10.2139/ssrn.2783647

Duriau, V. J., Reger, R. K., & Pfarrer, M. D. (2007). A content analysis of the content analysis literature in organization studies: Research themes, data

sources, and methodological refinements. *Organizational Research Methods*, *10*(1), 5–34.

Eisenmann, T., Parker, G., & Van Alstyne, M. (2011). Platform envelopment. *Strategic Management Journal*, *32*(12), 1270–1285.

Engel, C., & Rogers, J. H. (2004). European product market integration after the euro. *Economic Policy*, *19*(39), 348–384. https://doi.org/10.1111/j.1468-0327.2004.00126.x

Ensafi, R., Knockel, J., Alexander, G., & Crandall, J. R. (2015). Examining how the great firewall discovers hidden circumvention servers. *Proceedings of the 2015 ACM Conference on Internet Measurement Conference*, 445–458.

European Union. (2018). Regulation (EU) 2018/302 on addressing unjustified geo-blocking [Official Journal of the European Union].

Foss, N. J., & Saebi, T. (2017). Fifteen years of research on business model innovation: How far have we come, and where should we go? *Journal of Management*, *43*(1), 200–227. https://doi.org/10.1177/0149206316675927

Gilardi, F., Alizadeh, M., & Kubli, M. (2023). ChatGPT outperforms crowd workers for text-annotation tasks. *Proceedings of the National Academy of Sciences*, *120*(30), e2305016120. https://doi.org/10.1073/pnas.2305016120

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research: Notes on the gioia methodology. *Organizational Research Methods*, *16*(1), 15–31.

Główny Urząd Statystyczny (GUS). (2024). Average monthly gross wage and salary in enterprise sector [Central Statistical Office of Poland. Median estimated from average gross wage. Accessed: 2025-12-27]. https://stat.gov.pl/en/topics/labour-market/working-employed-wages-and-salaries-cost-of-labour/

Goldfarb, A., & Tucker, C. (2019). Digital economics. *Journal of Economic Literature*, *57*(1), 3–43.

Gomez-Herrera, E., Martens, B., & Alaveras, G. (2016). *Geo-blocking of audiovisual content in the EU digital single market* (tech. rep.). JRC Digital Economy Working Paper 2015-14. https://doi.org/10.2139/ssrn.2676060

Granados, N., Gupta, A., & Kauffman, R. J. (2006). Information transparency in business-to-consumer markets: Concepts, framework, and research agenda. *Information Systems Research*, *17*(2), 107–126.

Grand View Research. (2023). Virtual private network (VPN) market size, share & trends analysis report [Report ID: GVR-4-68039-164-2. Accessed: 2025-12-27].

GWI (GlobalWebIndex). (2023). VPN usage around the world: Statistics and trends [GlobalWebIndex annual report on digital consumer trends. Available at: https://www.gwi.com].

Hakimi Parizi, A., Liu, Y., Nokku, P., Gholamian, S., & Emerson, D. (2023). A comparative study of prompting strategies for legal text classification. *Proceedings of the Natural Legal Language Processing Workshop 2023*, 258–265. https://doi.org/10.18653/v1/2023.nllp-1.25

Hannak, A., Soeller, G., Lazer, D., Mislove, A., & Wilson, C. (2014). Measuring price discrimination and steering on e-commerce web sites. *Proceedings of the 2014 Conference on Internet Measurement Conference*, 305–318. https://doi.org/10.1145/2663716.2663744

Higgins, G. E., Wolfe, S. E., & Marcum, C. D. (2008). Digital piracy: An examination of three measurements of self-control. *Deviant Behavior*, *29*(5), 440–460. https://doi.org/10.1080/01639620701598023

IFRS Foundation. (2023). IAS 29 financial reporting in hyperinflationary economies [International Accounting Standards. Available at: https://www.ifrs.org/issued-standards/list-of-standards/ias-29-financial-reporting-in-hyperinflationary-economies/].

Ikram, M., Vallina-Rodriguez, N., Seneviratne, S., Kaafar, M. A., & Paxson, V. (2016). An analysis of the privacy and security risks of android vpn permission-enabled apps. *Proceedings of the 2016 Internet Measurement Conference*, 349–364.

INDEC. (2023). Average wages in argentina [Accessed: 2025-12-27].

Johnson, M. W., Christensen, C. M., & Kagermann, H. (2008). Reinventing your business model. *Harvard Business Review*, *86*(12), 50–59.

Karimi, J., & Walter, Z. (2020). Strategic agility, business model innovation and firm performance. *International Journal of Information Management*, *53*.

Kastanakis, M. N., & Balabanis, G. (2012). Between the mass and the class: Antecedents of the “bandwagon” luxury consumption behavior. *Journal of Business Research*, *65*(10), 1399–1407.

Laperdrix, P., Bielova, N., Baudry, B., & Avoine, G. (2020). Browser fingerprinting: A survey. *ACM Transactions on the Web*, *14*(2), 1–33.

Lindsay, D., & Ricketson, S. (2006). Copyright, privacy and digital rights management (DRM). In *New dimensions in privacy law* (pp. 121–153). Cambridge University Press. https://doi.org/10.1017/cbo9780511494208.007

Lobato, R. (2019). *Netflix nations: The geography of digital distribution*. New York University Press.

Masnick, M. (2019). The splinternet is already here.

MaxMind. (2021). GeoIP2 databases and web services [Technical Documentation. Accessed: 2025-12-27]. https://www.maxmind.com/en/geoip2-databases

Mi, X., Feng, X., Liao, X., Liu, B., Wang, X., Qian, F., Li, Z., Alrwais, S., Sun, L., & Liu, Y. (2019). Resident evil: Understanding residential IP proxy as a dark service. *Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP)*, 1009–1025. https://doi.org/10.1109/SP.2019.00011

Mihelcic, D., & Piatkivskyi, D. (2020). Decentralized VPN: The next generation of online privacy [Mysterium Network (BlockDev AG, Zug, Switzerland). Documentation available at: https://docs.mysterium.network. Source code at: https://github.com/mysteriumnetwork/node].

Milne, G. R., Culnan, M. J., & Greene, H. (2006). A longitudinal assessment of online privacy notice readability. *Journal of Public Policy & Marketing*, *25*(2), 238–249. https://doi.org/10.1509/jppm.25.2.238

Netflix. (2016). Netflix is now available around the world [Netflix Media Center press release, January 6, 2016. Available at: https://about.netflix.com/en/news/netflix-is-now-available-around-the-world].

Oberholzer-Gee, F., & Strumpf, K. (2007). The effect of file sharing on record sales: An empirical analysis. *Journal of Political Economy*, *115*(1), 1–42.

Odlyzko, A. (2003). Privacy, economics, and price discrimination on the internet. In *Economics of information security* (pp. 187–211). Springer. https://doi.org/10.1007/1-4020-8090-5_15

OECD. (2023). Average annual wages [OECD Employment and Labour Market Statistics. Accessed: 2025-12-27. Previously available at: https://data.oecd.org/earnwage/average-wages.htm]. https://data-explorer.oecd.org/vis?df[ds]=dsDisseminateFinalDMZ&df[id]=DSD_EARNINGS@DF_AV_AN_WAGE&df[ag]=OECD.ELS.SAE

Osterwalder, A., & Pigneur, Y. (2010). *Business model generation: A handbook for visionaries, game changers, and challengers*. John Wiley & Sons.

Pakistan Bureau of Statistics (PBS). (2024). Labour force statistics [Median wage estimated from Labour Force Survey. Accessed: 2025-12-27]. https://www.pbs.gov.pk/labour-force-statistics

Pakko, M. R., & Pollard, P. S. (2003). Burgernomics: A big mac guide to purchasing power parity. *Federal Reserve Bank of St. Louis Review*, *85*(6), 9–28.

Parker, G., & Van Alstyne, M. (2018). Innovation, openness, and platform control. *Management Science*, *64*(7), 3015–3032. https://doi.org/10.1287/mnsc.2017.2757

Pearson, K. (1895). Note on regression and inheritance in the case of two parents. *Proceedings of the Royal Society of London*, *58*, 240–242. https://doi.org/10.1098/rspl.1895.0041

Peukert, C., Claussen, J., & Kretschmer, T. (2017). Piracy and box office movie revenues: Evidence from Megaupload. *International Journal of Industrial Organization*, *52*, 188–215. https://doi.org/10.1016/j.ijindorg.2016.12.006

Philippine Statistics Authority (PSA). (2024). Current labor statistics: Wages and salaries [Median wage estimated from Labour Force Survey data. Accessed: 2025-12-27]. https://psa.gov.ph/statistics/labor-and-employment

Poort, J., & Zuiderveen Borgesius, F. J. (2019). Does everyone have a price? understanding people's attitude towards online and offline price discrimination. *Internet Policy Review*, *8*(1). https://doi.org/10.14763/2019.1.1383

Ransbotham, S., & Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research*, *20*(1), 121–139.

Reidenberg, J. R., Russell, N. C., Callen, A. J., Qasir, S., & Norton, T. B. (2015). Privacy harms and the effectiveness of the notice and choice framework. *I/S: A Journal of Law and Policy for the Information Society*, *11*, 485–535.

Reimers, I. (2016). Can private copyright protection be effective? evidence from book publishing. *The Journal of Law and Economics*, *59*(2), 411–440.

Rochet, J.-C., & Tirole, J. (2003). Platform competition in two-sided markets. *Journal of the European Economic Association*, *1*(4), 990–1029.

Rogoff, K. (1996). The purchasing power parity puzzle. *Journal of Economic Literature*, *34*(2), 647–668.

Security.org. (2023). Vpn statistics and usage [Accessed: 2025-12-27]. https://www.security.org/vpn/statistics/

Shapiro, C., & Varian, H. R. (1998). *Information rules: A strategic guide to the network economy*. Harvard Business Press.

Sinha, R. K., Machado, F. S., & Sellman, C. (2010). Don't think twice, it's all right: Music piracy and pricing in a DRM-free environment. *Journal of Marketing*, *74*(2), 40–54. https://doi.org/10.1509/jm.74.2.40

Srnicek, N. (2017). *Platform capitalism*. Polity Press.

State Statistics Service of Ukraine. (2024). Average monthly wages [Estimate based on pre-conflict wage data and inflation-adjusted projections. Accessed: 2025-12-27]. https://ukrstat.gov.ua/

Stiglitz, J. E. (2008). Economic foundations of intellectual property rights. *Duke Law Journal*, *57*, 1693–1724.

Sundararajan, A. (2004). Managing digital piracy: Pricing and protection. *Information Systems Research*, *15*(3), 287–308.

Swiss Federal Statistical Office. (2023). Switzerland average monthly gross wage [Accessed: 2025-12-27]. https://tradingeconomics.com/switzerland/wages

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review*, *22*(6), 664–670.

Teece, D. J. (2010). Business models, business strategy and innovation. *Long Range Planning*, *43*(2-3), 172–194.

Thaler, R. H., & Sunstein, C. R. (2003). Libertarian paternalism. *American Economic Review*, *93*(2), 175–179. https://doi.org/10.1257/000282803321947001

Thongmak, M. (2017). Ethics, neutralization, and digital piracy. *International Journal of Electronic Commerce Studies*, *8*(1), 1–24. https://doi.org/10.7903/ijecs.1436

Tirole, J. (1988). *The theory of industrial organization*. MIT Press.

Trimble, M. (2024). Introduction to geo-blocking. In *The EU geo-blocking regulation* (pp. 1–59). Edward Elgar Publishing. https://doi.org/10.4337/9781803923871.00008

Turkish Statistical Institute. (2023). Turkey average gross wage [Accessed: 2025-12-27]. https://tradingeconomics.com/turkey/wages

Varian, H. R. (1989). Price discrimination. *Handbook of Industrial Organization*, *1*, 597–654.

Waldfogel, J. (2010). Music file sharing and sales displacement in the iTunes era. *Information Economics and Policy*, *22*(4), 306–314. https://doi.org/10.1016/j.infoecopol.2010.02.002

Wasko, M. M., & Faraj, S. (2005). Why should I share? examining social capital and knowledge contribution in electronic networks of practice. *MIS Quarterly*, *29*(1), 35–57.

Weckbach, T. (2025). VPN data extraction and analysis: Source code and dataset repository [GitHub repository containing the complete data collection pipeline, Gemini-based classification scripts, analysis code, and the master dataset used in this thesis].

Winter, P., Pulls, T., & Fuss, J. (2013). ScrambleSuit: A polymorphic network protocol to circumvent censorship. *Proceedings of the 12th ACM Workshop on Privacy in the Electronic Society*, 213–224. https://doi.org/10.1145/2517840.2517856

Wirtz, B. W., Pistoia, A., Ullrich, S., & Göttel, V. (2016). Business models: Origin, development and future research perspectives. *Long Range Planning*, *49*(1), 36–54.

World Bank. (2023). World development indicators: Income distribution [World Bank Open Data. Available at: https://data.worldbank.org/indicator].

Xia, L., Monroe, K. B., & Cox, J. L. (2004). The price is unfair! a conceptual framework of price fairness perceptions. *Journal of Marketing*, *68*(4), 1–15. https://doi.org/10.1509/jmkg.68.4.1.42733

Zhu, F., & Iansiti, M. (2012). Entry into platform-based markets. *Strategic Management Journal*, *33*(1), 88–106. https://doi.org/10.1002/smj.941

Zott, C., Amit, R., & Massa, L. (2011). The business model: Recent developments and future research. *Journal of Management*, *37*(4), 1019–1042.

Zuiderveen Borgesius, F. J., & Poort, J. (2017). Online price discrimination and EU data privacy law. *Journal of Consumer Policy*, *40*(3), 347–366. https://doi.org/10.1007/s10603-017-9354-z

List of Figures

1. Visualizing the Classification Gap: Proportional Category Distribution Between Models (sorted by Gemini share). 34

2. Total Clause Counts by Company. The dataset is weighted towards Microsoft and YouTube due to the complexity and length of their multiple policy documents. 38
3. Distribution of Data by Document Type. Annual Reports (10-K) and Earnings Calls provide the bulk of strategic context, while ToS documents provide the specific enforcement clauses. 39
4. Proportional Distribution of Enforcement Categories (Aggregate) . 43
5. The Fortress Index: Percentage of Enforcement Clauses (Technical Blocking + Legal Threat) as a Share of Strategic Sentences per Service 44
6. The Affordability Gap: Digital Service Cost as Percentage of Local Monthly Income. Darker red indicates higher relative cost for local citizens. 46
7. Strategic Alignment: Comparison of Price Discrimination scores vs. Enforcement Intensities across analyzed services. 49
8. Temporal Evolution of Category Incident Counts (Aggregate, Excluding VPN Providers) 50
9. Evolution of Strategic Frames over Time (Excluding General Terms and VPN Providers) 51

10. Strategic Framing by Company: Macro-Category Distribution. VPN providers (ExpressVPN, NordVPN) show the highest proportion of coercive/legal framing (CRL $>$ 60%), while software companies (Microsoft, Adobe) and streaming platforms overwhelmingly use business model adaptation framing (BMA $>$ 70%). 54

11. The Adversarial Timeline: Coercive Barriers vs. Technical Circumvention (2020–2025). Events above the timeline reflect corporate enforcement measures documented in the ToS analysis; events below the timeline represent circumvention technologies. 60
12. Strategic Evolution: Video Streaming Leaders (2020–2025). Grouping Netflix, YouTube, Disney+, and Amazon Prime. 61
13. Strategic Evolution: Music Streaming (2020–2025). Compared with the video streaming leaders in Figure 12, music services show markedly lower Technical Blocking intensity. Spotify shows zero Technical Blocking clauses across the entire period, while Apple Music shows only intermittent spikes. 62
14. Strategic Evolution: Software Utilities (2020–2025). Microsoft and Adobe show distinct patterns from streaming services, relying more on Regulatory Compliance and Legal Threats than Technical Blocking. 63
15. Distribution of Policy Text Categories Over Time (Strategic Categories Only). 66

16. Evolution of VPN Provider Enforcement. Note: Specific VPN graphs have been excluded for brevity as they show minimal variation. . 81
17. Absolute Sentence Counts: Video and Music Streaming (2020–2025). Unlike the proportional charts in Chapter 5, this figure shows raw sentence counts to illustrate the volume of enforcement language. 82
18. Absolute Sentence Counts: Software Utilities (2020–2025). . . . 83

List of Tables

1. Model Comparison: Gemini 3 Flash vs. Zero-Shot BERT Classification. Categories with $< 0.2\%$ share in both models (Security Risk, User Workaround) are omitted for clarity; column percentages therefore do not sum to exactly 100%. 33
2. Absolute Category Counts by Service. YouTube dominates Technical Blocking (N=94), while streaming services rely heavily on Content Licensing. 39
3. Complete DSPI Summary by Country. PTW = average subscription cost across all available services as % of median monthly wage. Lower DSPI indicates cheaper markets relative to the US baseline. 40
4. Complete DSPI Matrix: Per-Service Price Index by Country (US = 1.00). Values < 0.50 are highlighted as high-arbitrage opportunities. 41
5. Monthly Subscription Prices in USD Across All Services and Countries (December 2025). Microsoft 365 and NordVPN/ExpressVPN show the equivalent monthly cost derived from annual/multi-year plans. 42
6. Raw Count of Enforcement Incidents per Service (2020–2025) . . 45
7. Price Discrimination Score, Enforcement Intensity, and Their Correlation. The full-sample Pearson $r \approx -0.55$ ($p = 0.10$) is driven primarily by VPN providers (low PD, high EI) and is not statistically significant at conventional thresholds. Excluding VPNs ($N = 8$), the correlation reverses to a weak positive $r \approx +0.35$ ($p = 0.40$), suggesting a temporary trend where higher price discrimination relates with slightly higher enforcement among digital service providers, though neither result is statistically significant. Given the small sample sizes, these correlations should be interpreted as exploratory pattern observations. 48

8. Complete Fortress Index Ranking. VPN providers score highest due to their security-focused framing, followed by YouTube and Microsoft with active enforcement strategies. 51
9. Absolute Category Counts by Year Across All Services (2020–2025). Technical Blocking peaks sharply in 2023, coinciding with YouTube's enforcement escalation. 52

10. Median Monthly Wages and Exchange Rates Used for PTW Calculations (December 2025). Countries are ordered by USD wage (descending). 84
11. Complete PTW Matrix: Subscription Cost as % of Median Monthly Wage by Service and Country (December 2025). Cells marked "–" indicate the service is unavailable in that country. Values $\geq 10\%$ are highlighted in **bold**. 85

Glossary and Acronyms

Glossary

digital geo-arbitrage A subset of geo-arbitrage specific to digitally delivered subscription services (e.g., streaming, cloud storage, SaaS), where the intangible nature of the product eliminates shipping costs and physical border controls, making price discrimination both easier to implement and easier to circumvent via VPN or proxy tools. 2, 7

discrimination dilemma The paradox that the more aggressively a firm discriminates on price across regions, the greater the arbitrage incentive it creates and the higher the enforcement costs required to maintain market segmentation. 8

geo-arbitrage The practice of exploiting geographic price differences for digital services by using VPNs or similar tools to purchase subscriptions at prices intended for a different (typically lower-income) market; used synonymously with “price hopping” and “subscription hopping” in this thesis. 98

Acronyms

BMA Business Model Adaptation & Pricing. 53, 54, 94

BMI Business Model Innovation. 2, 16, 18, 21, 56, 76, 77

CDN Content Delivery Network. 17

CRL Coercive Restriction & Legal Threat. 53, 54, 94

DPI Deep Packet Inspection. 64

DRM Digital Rights Management. 2, 14, 59

DSPI Digital Services Price Index. 2, 4, 9, 12, 21–24, 26, 35, 37–41, 45–49, 53, 57, 58, 69, 71, 74, 76, 80, 84, 96, 100

dVPN Decentralized Virtual Private Network. 79

EU European Union. 29, 68, 69, 78, 80

GCO General Corporate Operations. 54

GDPR General Data Protection Regulation. 69

LLM Large Language Model. 2, 23, 27, 28, 31, 33–35, 72–74, 76, 80, 100

NLI Natural Language Inference. 27, 73, 76

PPP Purchasing Power Parity. 3, 11, 12, 26

PTW Price-to-Wage. 2, 9, 22, 23, 26, 39, 40, 47, 74, 76, 84, 96, 97

RQ Research Question. 3, 9, 23, 24, 27, 74, 75

SaaS Software as a Service. 59, 71, 80

ToS Terms of Service. 2, 9, 15, 20, 23, 25, 27, 31, 34, 36, 39, 44, 49, 51, 53, 63, 65, 69, 72, 76, 94, 100

VPN Virtual Private Network. 2, 6–8, 11, 13–15, 17, 18, 20, 21, 24, 25, 28, 29, 36, 38–42, 44, 46, 47, 49–54, 56–58, 60–65, 67, 69, 70, 72, 75, 79, 81, 94–98

Declaration on the Use of AI-Based Tools

In accordance with the guidelines of TU Darmstadt on the use of generative AI in academic work, the following AI-based tools were used during the preparation of this thesis. All AI-generated outputs were critically reviewed, verified against primary sources, and adapted by the author. No content was adopted without independent verification. The intellectual contribution, argumentation, and all scientific conclusions remain entirely the author's own work.

Google Gemini 3 Pro Used for ideation and brainstorming during the early conceptual phase of the research design. Outputs served as discussion prompts and were not adopted verbatim.

Google Gemini 3 Flash Used as the classification engine in the LLM-based ToS analysis pipeline (see Section 3.3.2). The model processed approximately 25,000 sentences from corporate documents. The system prompt, parameters, and validation procedure are fully documented in the methodology chapter.

Anthropic Claude (Opus 4.5 and Opus 4.6) Used as a coding assistant for the development of the Python-based data collection and analysis scripts (web scraping, DSPI calculation, visualization). All code was reviewed, tested, and debugged by the author.

Erklärung zur Abschlussarbeit gemäß § 22 Abs. 7 APB TU Darmstadt

Hiermit erkläre ich, Tim Weckbach, dass ich die vorliegende Arbeit gemäß § 22 Abs. 7 APB der TU Darmstadt selbstständig, ohne Hilfe Dritter und nur mit den angegebenen Quellen und Hilfsmitteln angefertigt habe. Ich habe mit Ausnahme der zitierten Literatur und anderer in der Arbeit genannter Quellen keine fremden Hilfsmittel benutzt. Die von mir bei der Anfertigung dieser wissenschaftlichen Arbeit wörtlich oder inhaltlich benutzte Literatur und alle anderen Quellen habe ich im Text deutlich gekennzeichnet und gesondert aufgeführt. Dies gilt auch für Quellen oder Hilfsmittel aus dem Internet.

Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Mir ist bekannt, dass im Falle eines Plagiats (§ 38 Abs. 2 APB) ein Täuschungsversuch vorliegt, der dazu führt, dass die Arbeit mit 5,0 bewertet und damit ein Prüfungsversuch verbraucht wird. Abschlussarbeiten dürfen nur einmal wiederholt werden.

Bei einer Thesis des Fachbereichs Architektur entspricht die eingereichte elektronische Fassung dem vorgestellten Modell und den vorgelegten Plänen.

Darmstadt, 17.02.2026

Tim Weckbach