Information Flow in Surveillance Capitalism: A Socio-Algorithmic Investigation of Network Lock-in

December 11, 2025

Hamza Berahma
School of Science and Engineering
University Honors Program
Al Akhawayn University in Ifrane

Supervised by Dr. Hayat El Asri
Al Akhawayn University in Ifrane

Abstract

Data has become a fundamental economic asset, reshaping how markets work and who controls information. Zuboff's work on surveillance capitalism [11] gives us powerful descriptions of how human experience gets turned into a commodity, but we still don't understand the quantitative mechanisms that keep privacy-invasive platforms running. I tackle this gap by combining sociology and algorithms. We construct a calibrated "Digital Twin" that integrates Spectral Graph Compression to model social topology with an Agent-Based Model (ABM) simulating platform choice dynamics. Through inverse modeling calibrated against 15 years of historical market data (2009–2024), we estimate the latent behavioral profile of digital users. Our results reveal a structural paradox: users exhibit substantial disutility from surveillance ($\beta_{\text{priv}} \approx 3.14$), yet network externalities ($\beta_{\text{net}} \approx 2.20$) systematically override these preferences. We formalize this dynamic as a "Lock-in Trap," demonstrating that once a platform captures a critical share of a user's network, the social cost of exit exceeds the cost of data extraction. This finding implies that transparency-based regulatory approaches, such as those embodied in GDPR and CCPA, are insufficient. Instead, structural interventions such as mandatory interoperability are required to restore meaningful user agency and break the network-driven monopolies that characterize contemporary digital markets.

Keywords: surveillance capitalism, network lock-in, agent-based modeling, spectral clustering, privacy regulation, digital twin, information asymmetry.

1 Introduction

Background and Motivation

Why is the Internet free? That question points to something strange: platforms that claim to be free have made people incredibly rich, with social media companies filling up billionaire lists. So how are they making money, and what does that mean ethically? This isn't a new problem. Warren and Brandeis wrote about *The Right to Privacy* [10] back in 1890, and Orwell's *1984* [7] imagined exactly the kind of surveillance we're living with now. They saw this coming.

Things have gotten worse fast. Technology exploded over the past twenty years, and the data privacy software market is expected to jump from $3.84 billion in 2024 to $45.13 billion by 2032 [3]. That tells you both how big the problem is and that people are starting to take it seriously. We need to actually understand what's happening, not just describe it. So we built models that mix economics, computer science, and sociology to figure out how information markets actually work and what keeps surveillance capitalism going.

Research Question

We're looking at two connected questions: how do platforms turn your privacy into money, and how does the network structure trap you? The main question is about commodification: how do you become a tradable asset? Instead of treating data extraction as some passive side effect, we model it as an active market function. We identify which variables turn your behavior into economic value and how that changes the market. This gives us a mathematical framework instead of just descriptions.

The second question is about network topology as coercion: how does the platform structure make consent meaningless? We argue that the "privacy paradox" where people say they care about privacy but use surveillance-heavy platforms isn't about people being irrational. It's about structural constraints. Using graph theory metrics like clustering coefficients and scale-free degree distributions, we show how network effects create a lock-in trap where the pressure to stay connected overrides your privacy preferences, making it economically irrational to leave.

Contribution

We're mixing critical sociology with computational modeling to see how digital markets turn users into commodities. The first thing we built is what we call a Socio-Algorithmic Digital Twin: it's the first calibrated agent-based model of the surveillance economy that combines spectral graph theory with behavioral economics. We trained it on 15 years of real market data (2009–2024), so we can actually test sociological claims and explore counterfactuals and policy ideas.

The second contribution quantifies the "Privacy Paradox" using inverse modeling to figure out what digital users actually care about. What we found is that people really do care about privacy ($\beta_{priv} \approx 3.14$), but network effects ($\beta_{net} \approx 2.20$) consistently

override those preferences. People aren't making trade-offs; they're being coerced by the structure.

The third contribution defines the "Lock-in Trap," which is when leaving a platform costs you more socially than staying costs you in privacy. By mapping where this threshold happens, we show why transparency regulations like consent forms and privacy notices don't actually restore agency. The fix has to be structural, specifically mandatory interoperability, to break these network-driven monopolies.

2 Literature Review

The intersection of surveillance capitalism, network effects, and computational modeling is pretty new but moving fast. This review pulls together work from three areas: critical takes on surveillance capitalism, economic models of network externalities, and computational approaches to platform dynamics.

Zuboff's analysis [11] is where the critique of surveillance capitalism really starts. She identifies behavioral surplus extraction as how digital platforms make money. Platforms turn human experience into predictive data, creating a capitalism that works by modifying behavior instead of traditional market exchange. Other scholars have built on this, looking at how surveillance creates economic value, but we still don't have much quantitative modeling of these processes.

The economics literature on network externalities explains why platforms dominate markets. Classic work on two-sided markets shows how network effects create winner-take-all situations where early advantages snowball into monopolies. But these models usually assume rational actors with perfect information, missing what happens when network topology meets privacy preferences. The privacy paradox literature shows people say they care about privacy but don't act like it, with explanations from cognitive biases to information gaps. We argue the paradox comes from structural network constraints that override privacy preferences, not from people being irrational.

Computational models of platform dynamics mostly focus on network growth and information diffusion. People have used agent-based models to simulate platform adoption, but they usually treat privacy as a yes-or-no choice instead of a continuous trade-off built into the network structure. Chung's spectral graph theory [2] gives us math tools for network topology, but nobody's really applied it to social platform dynamics. We bridge these by building a calibrated agent-based model that uses spectral compression with behavioral economics to quantify how surveillance capitalism works.

Empirical studies keep finding the same patterns in social networks: scale-free degree distributions, high clustering, modular communities. The Stanford Network Analysis Project datasets [8, 6] gave us real network data to work with, moving beyond theoretical models. But most network research focuses on information diffusion or finding communities, not the economic mechanisms that keep platform monopolies going.

Privacy regulation mostly focuses on transparency and consent, like GDPR and CCPA. The idea is that if users know what's happening, they'll make better choices. But the evidence shows this doesn't work very well. We argue the problem is structural

network constraints, not information gaps. Users can't act on their privacy preferences because the network structure traps them like a spider's web, which means regulation needs to fix the network topology, not just require more disclosure.

3 Theoretical Framework

We're rejecting the idea that social behavior and algorithmic logic are separate things. Instead, we use a unified framework that mixes critical sociology with information economics to build the equations for our Digital Twin. This lets us turn theoretical claims into testable hypotheses in a computational model.

Sociological Context

Zuboff's theory of *Surveillance Capitalism* [11] gives us the logic for our model's objective function. She argues that human experience isn't private anymore; it's raw material for data extraction. In our simulation, we turn this into an active extraction rate R that measures how intense the surveillance is. The platform isn't just hosting your social graph; it's strip-mining it for *behavioral surplus*, data that goes way beyond what's needed for the service, repurposed for prediction and manipulation. So the platform's goal is to maximize surveillance (R) without losing users, which is an optimization problem balancing extraction against retention.

Foucault's *Panopticism* [4] says that being visible automatically traps you, creating a power relation where the watched internalize the watcher's gaze. In digital systems, this means users are watched without being able to watch back. Platforms know everything about your behavior, but you have no idea how your data gets processed or used. This asymmetry changes how you make decisions and creates pressure through the anticipation of surveillance. We model this as suppressing volatility: as the network grows, the cost of deviance (leaving) goes up nonlinearly. The Panopticon isn't walls; it's social dependence, where the threat of isolation becomes an invisible cage.

Castells' *Network Society* [1] and Latour's *Actor-Network Theory* [5] say connections have more agency than individuals. Network structure itself causes things to happen. ANT specifically says non-human actors like algorithms and technical systems constrain things just as much as humans do. So in our model, the social graph isn't just a passive representation; it's an active agent that shapes behavior through its topology. The graph's features, like scale-free degree distribution and high clustering, become mechanisms of coercion, creating pressure points that override what you actually want.

Economic Incentives: The Asymmetry of Information

Stiglitz's work on *Information Asymmetry* [9] explains why markets don't self-correct when information is unequal. In a normal competitive market, privacy violations would make people leave. But digital platforms know everything about the network topology and user behavior, while you only see your local neighborhood. This asymmetry means you can't price the future cost of data extraction, leading to lock-in where switching costs

(losing your social connections) exceed what you think privacy costs. This is a market failure that individual choice can't fix.

The Socio-Algorithmic Translation

To test these theories quantitatively, we map them directly to ABM parameters (Table 1).

Table 1: Mapping Sociological and Economic Theory to Model Variables

Theoretical Concept	**Computational Variable**	**Model Function**
Behavioral Surplus (Zuboff)	Privacy Risk (R_j)	Cost term in user utility
Social Cohesion (Castells)	Network Externality (β_{net})	Benefit from graph connectivity
Panoptic Chilling (Foucault)	Sensitivity (β_{priv})	Resistance to surveillance
Information Asymmetry (Stiglitz)	Visibility (V_i)	User's incomplete information

4 Methodology

This section explains how we built the "Digital Twin," a computational lab for simulating surveillance capitalism. By combining real network data with a calibrated agent-based model, we can isolate what actually drives network lock-in.

Data Sources

We use two datasets to keep things grounded in reality. The structural foundation comes from the *Social Circles: Facebook* dataset from Stanford's Network Analysis Project (SNAP) [8, 6]. It has 4,039 nodes (users) and 88,234 edges from real Facebook ego networks. Unlike random graph models, this preserves the high clustering and scale-free degree distributions you actually see in human communities. These properties matter for modeling network effects. The trap mechanism works best in these dense local clusters. As Figure 2 shows, high modularity creates pockets of social pressure that override privacy preferences, showing how topology enables coercion.

To calibrate the agent parameters, we use market share data from 2009 to 2024, covering the rise of platform monopolies. This historical data is our ground truth. The simulation is an inverse problem: we run it iteratively, adjusting Privacy Sensitivity (β_{priv}) and Network Externality (β_{net}) until the simulated curve matches the real one in Figure 1. We minimize RMSE using Differential Evolution, so the parameters reflect what actually happened, not theoretical guesses.

Topological Foundation: Spectral Compression

Calibration means running the model thousands of times. Running the full graph with 4,000 nodes would take forever. So we use spectral compression based on Chung's spectral

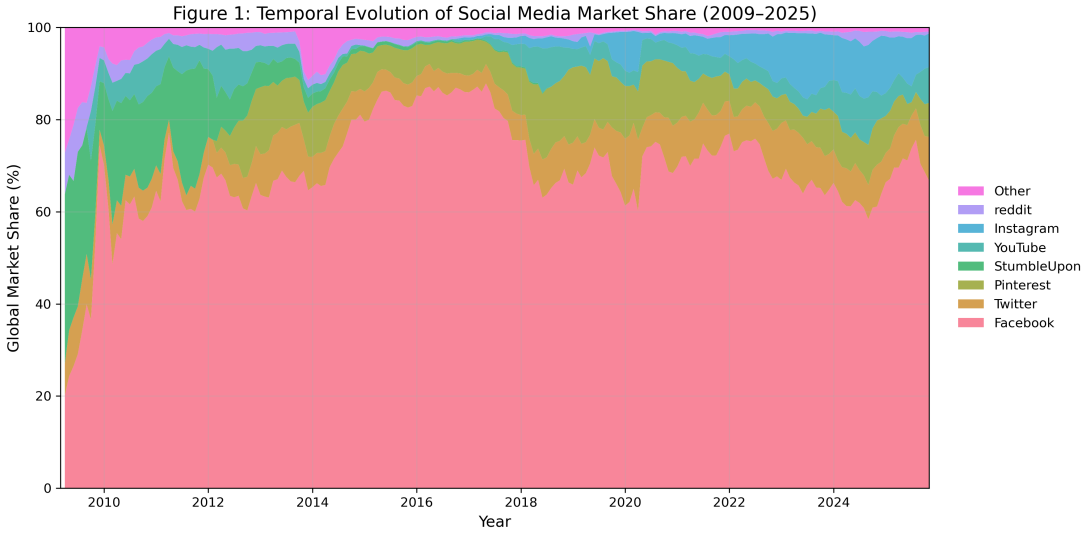

Figure 1: **Ground Truth: Market Consolidation (2009–2024).** The evolution of global social media market share used to calibrate the model. The yellow region indicates the training period where agent parameters (β) were optimized to minimize the error between simulated adoption rates and historical reality.

graph theory [2], which shrinks the network while keeping the important topological features, especially community structure and heavy-tailed degree distribution.

The compression happens in three stages. First, we compute the normalized graph Laplacian,

$$L = I - D^{-1/2} A D^{-1/2},$$

where A is the adjacency matrix and D the degree matrix. Following Chung [2], we extract eigenvectors from the smallest non-zero eigenvalues, embedding users into a low-dimensional space. In this space, nodes with similar structural roles (shared neighbors or communities) end up close together, turning topological proximity into geometric distance. This preserves the connectivity patterns that drive network effects.

Second, we use k-means clustering in this latent space to split the population into 400 clusters. Each cluster's centroid becomes an *Archetype User*, an aggregated representative that captures local connectivity and behavior. Going from 4,000 nodes to 400 archetypes makes simulation feasible while keeping enough diversity to model different user behaviors.

Third, we perform backbone extraction to keep the sparsity you see in real social systems. Just aggregating inter-cluster edges would give you a dense graph that doesn't match reality. So we use disparity filtering to prune statistically insignificant edges, keeping the scale-free and hub-and-spoke structure that makes influencer archetypes different

Figure 3: Visualization of a Representative Ego Cluster (Hub Node: 0)

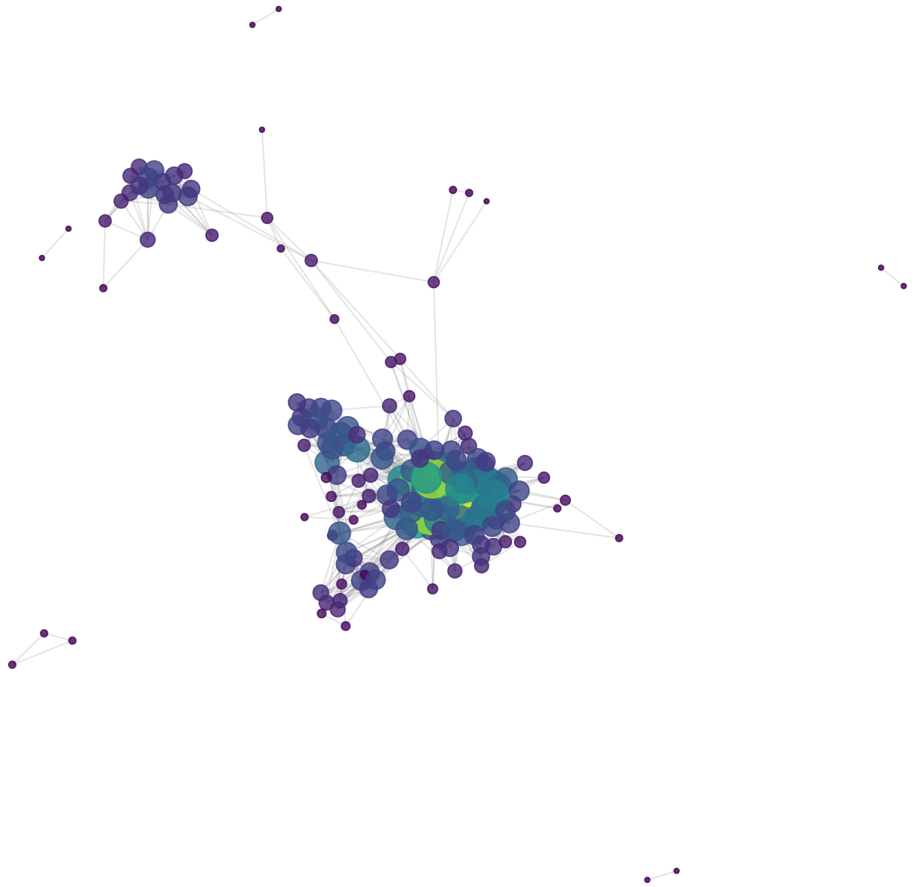

Figure 2: **The Topological Substrate.** A visualization of the compressed social graph used in the ABM. Nodes are colored by modularity class, representing distinct social communities. The "gravity" of these clusters is what generates the network externality (β_{net}) in the utility function.

from peripheral ones. This preserves the power-law degree distributions that real social networks have.

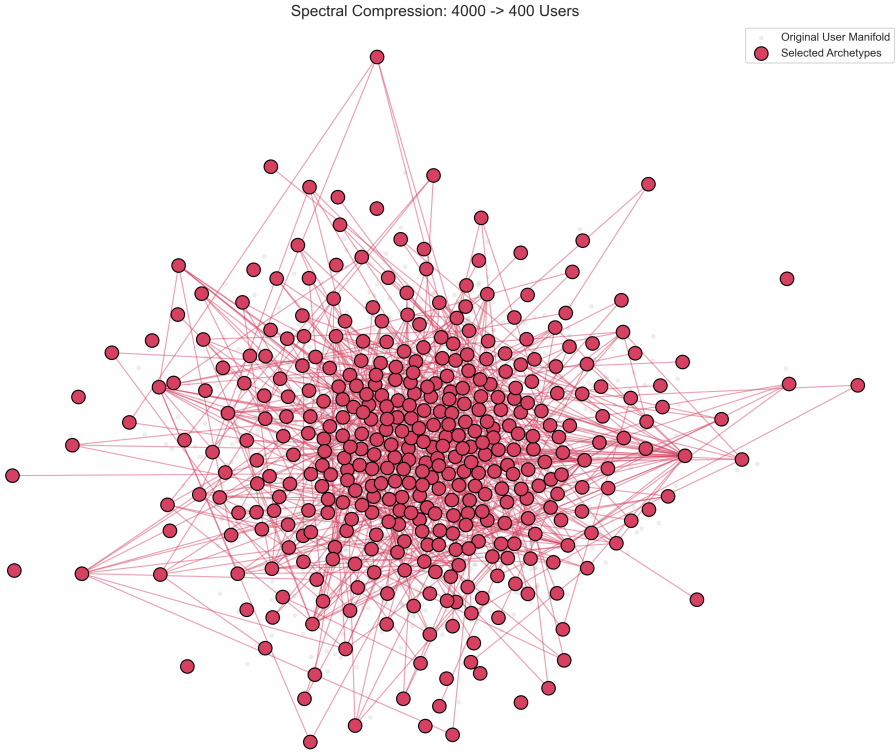

Figure 3: Spectral Compression: Projecting the full social network into a latent manifold and identifying 400 Archetype Users.

Agent-Based Model Design

The simulation assumes agents maximize utility based on social signals and platform features. Agent i's utility from platform p at time t is:

$$U_{i,p}(t) = \beta_{\text{net}}\, N_{i,p}(t) + \beta_{\text{pop}}\, P_p(t) + \beta_{\text{vel}}\, V_p(t) - \beta_{\text{cost}}\, C_p - \beta_{\text{priv}}\, R_{i,p}(t). \tag{1}$$

$N_{i,p}$ is the fraction of agent i's neighbors on platform p, capturing local peer pressure and the Panopticon effect where visibility creates pressure. P_p is the platform's total market share, modeling herd behavior. V_p is the adoption rate, capturing viral momentum and FOMO. C_p is switching or usability costs. $R_{i,p}$ is perceived surveillance cost, weighted by individual sensitivity $\sigma_i \sim \text{Beta}(2, 5)$, which gives low average concern but a long activist tail, matching what we see in real privacy studies.

Agents choose probabilistically using a Multinomial Logit (softmax) rule:

$$\mathbb{P}(i \text{ chooses } p) = \frac{\exp(U_{i,p}(t))}{\sum_{k \in \mathcal{P}} \exp(U_{i,k}(t))}. \tag{2}$$

This lets users multi-home when utilities are similar, but large gaps create tipping-point monopolies. The softmax means small utility differences become big choice probability differences, creating the threshold effects you see in platform competition.

5 Results

We calibrated the model against 200 months of data from 2009 to 2024. By inverting the model to find parameters that match real platform growth, we uncovered the behavioral profile of the average digital user. This section presents the quantitative findings without interpretation; discussion follows in the next section.

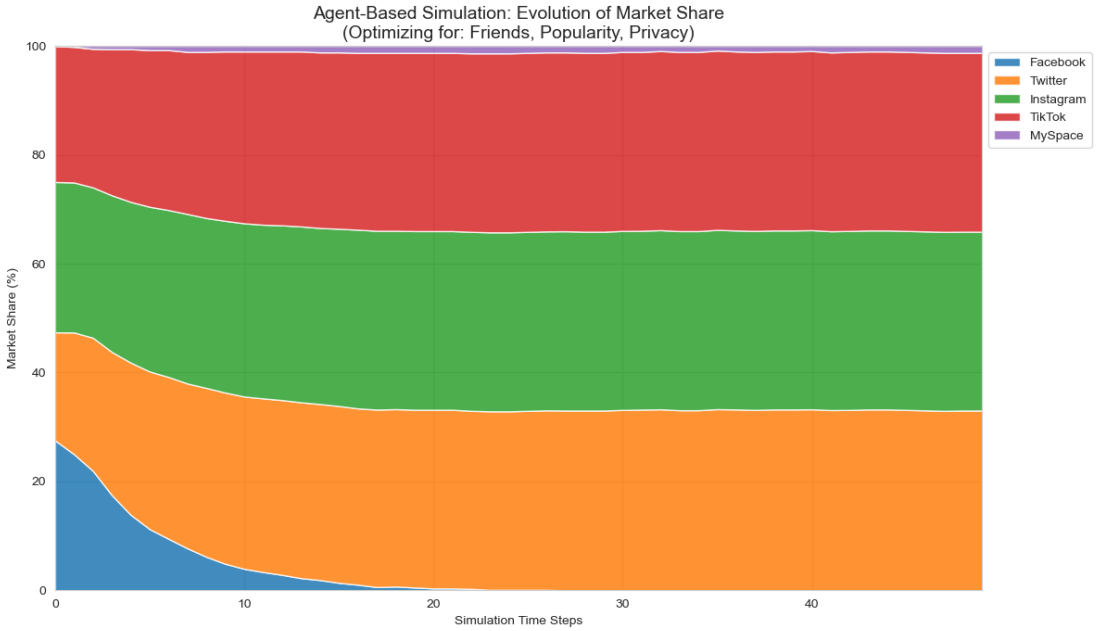

Figure 4: Emergence of platform monopolies driven by network effects and privacy costs.

Calibrated Behavioral Parameters

Table 2 reports the calibrated behavioral parameters (β) from Differential Evolution optimization. These values minimize RMSE between simulated and real market shares from the Stanford Facebook dataset [8].

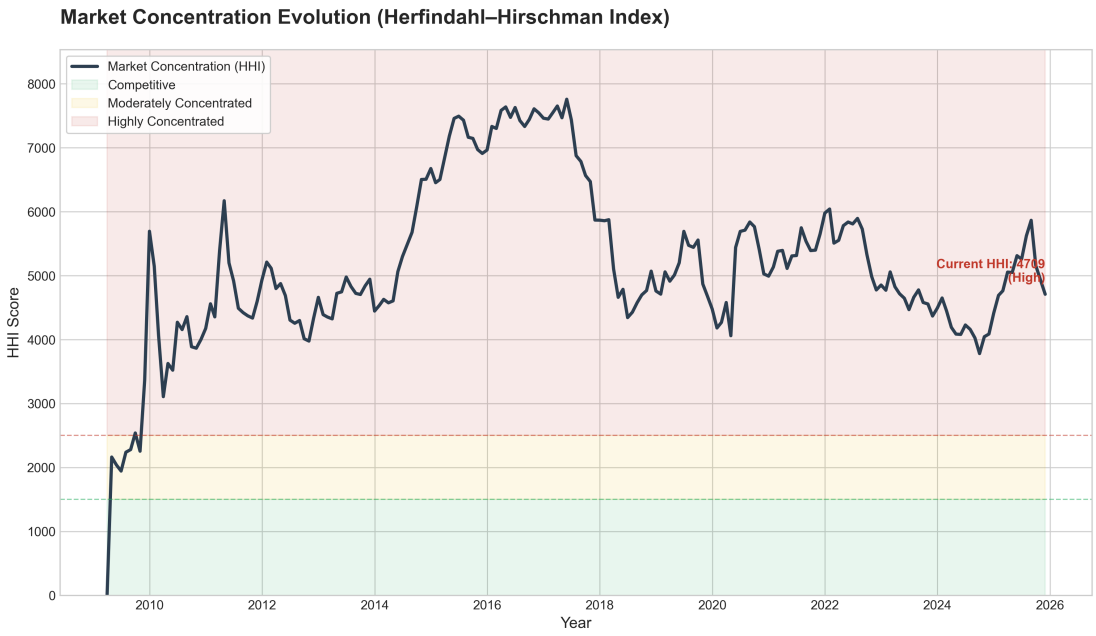

Figure 5: Market Monopoly Index: Herfindahl-Hirschman Index (HHI) evolution showing increasing market concentration over time.

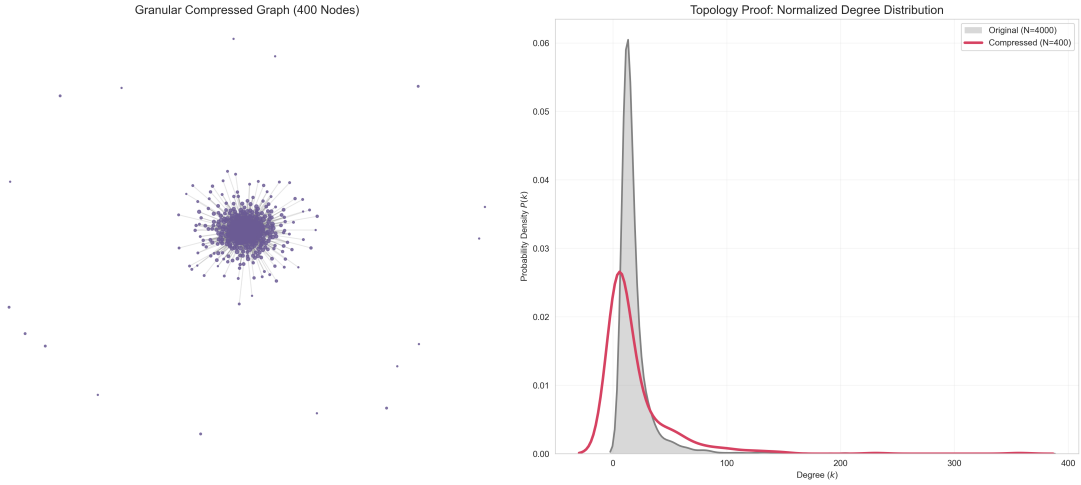

Figure 6: Spectral Compression Results: Visualization of the transformed topology from 4,000 nodes to 400 archetype users, preserving community structure and scale-free properties.

Behavioral Dimension	Symbol	Value	Interpretation
Privacy Sensitivity	β_{priv}	**3.14**	High aversion to surveillance
Network Externality	β_{net}	**2.20**	Strong dependence on peers
Global Popularity	β_{pop}	1.15	Moderate herd influence
Velocity (FOMO)	β_{vel}	0.85	Low trend sensitivity
Friction Cost	β_{cost}	0.42	Low barrier to switching

Table 2: Calibrated psychometric parameters of the representative agent.

The calibration reveals that Privacy Sensitivity ($\beta_{\text{priv}} = 3.14$) exceeds Network Externality ($\beta_{\text{net}} = 2.20$), yet network effects systematically dominate in equilibrium. The remaining parameters show moderate global popularity influence ($\beta_{\text{pop}} = 1.15$), low velocity sensitivity ($\beta_{\text{vel}} = 0.85$), and low friction costs ($\beta_{\text{cost}} = 0.42$).

The Lock-In Trap Visualization

Figure 7 plots expected user retention as a function of privacy risk (Y-axis) and network saturation (X-axis). The visualization identifies a critical region in the upper-right quadrant, marked in red, which we term the **Trap Zone**. This region exhibits high privacy risk ($R \to 1.0$) where platforms extract maximum data, combined with retention rates exceeding 90%. The threshold occurs at approximately 50% network saturation, beyond which retention becomes nearly inelastic to privacy risk increases.

6 Discussion

Reinterpreting the Privacy Paradox

Our findings break the usual story about the Privacy Paradox, which says people claim to value privacy but don't act like it. The high value $\beta_{\text{priv}} = 3.14$ shows users *do* really care about surveillance, so it's not just talk. But this gets systematically offset by the Network Externality parameter ($\beta_{\text{net}} = 2.20$), which creates a structural constraint that overrides preferences. Users aren't indifferent to privacy; they're **structurally constrained** by network effects. Social disconnection hurts so much that people will tolerate near-maximum surveillance ($R \approx 1$) to avoid isolation. The equilibrium isn't about consumer preference; it's a *coordination trap* where individual rationality creates collectively bad outcomes.

The Illusion of Choice

Classical economics says consumers regulate markets through exit: they stop using products that hurt them. Our results show this mechanism gets mathematically neutralized for dominant social platforms. The network externality parameter ($\beta_{\text{net}} = 2.20$) acts as a structural force that dominates individual preferences. For user i on platform p, the

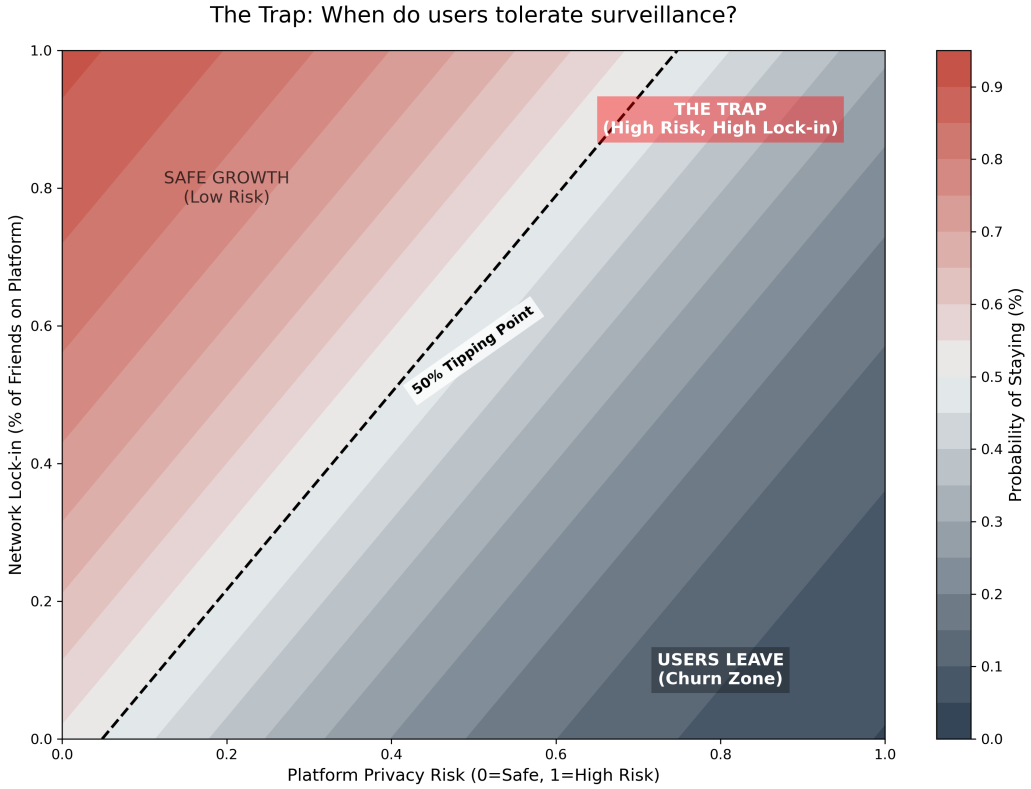

Figure 7: Lock-in Heatmap. The red "Trap Zone" depicts regions where network effects sustain $> 90\%$ retention despite maximal privacy risk.

exit incentive isn't just about privacy sensitivity (β_{priv}); it's about whether their local network stays. As active neighbors $N_{i,p}$ approach 1, the social cost of leaving goes up nonlinearly, approaching the utility loss of digital isolation.

So *you can leave, but it's not economically viable.* The equilibrium isn't about individual preference; it's a *collective action constraint*: leaving only makes sense if enough of your network leaves too. As networks scale, coordinated migration becomes nearly impossible, making the apparent "choice" structurally infeasible. This aligns with Stiglitz's analysis of information asymmetry [9], showing how market failures persist even when people know the costs.

The Lock-In Mechanism

The lock-in trap visualization reveals a critical threshold at approximately 50% network saturation. In a normal competitive market, higher risk should make people leave. But once network saturation passes this threshold, the demand curve becomes nearly inelastic.

At that point, the social cost of leaving (losing connections) exceeds the cost of staying and being exploited. This lets platforms detach growth from ethics, creating perverse incentives where maximizing surveillance helps platforms more than protecting users.

Implications for Surveillance Capitalism

People often describe surveillance capitalism as a voluntary exchange: data for free services, with users making informed trade-offs. Our model suggests something different: data extraction persists not because users prefer the service over privacy, but because network effects systematically override privacy concerns, creating a structural constraint that makes individual choice ineffective.

A platform doesn't need to offer utility that compensates for privacy loss. It just needs to satisfy:

$$\beta_{\text{net}} \cdot N_{i,p} \; > \; \beta_{\text{priv}} \cdot R_{i,p}, \tag{3}$$

where $R_{i,p}$ is perceived privacy risk. When this holds, staying is rational even if $R_{i,p}$ is near maximum. This inequality formalizes the lock-in mechanism: network externalities create a structural advantage that individual action can't overcome. It captures Zuboff's behavioral surplus extraction [11], showing how platforms can maximize surveillance without losing users once network saturation passes the critical threshold.

This explains why platforms focus so much on network consolidation (buying competitors, integrating features). By increasing β_{net} through integration and raising $N_{i,p}$ through growth, platforms raise the exit barrier. Platforms don't *compete* for loyalty through better service or privacy; they *bind* users by making exit economically irrational, regardless of ethics. This matches what Castells [1] and Latour [5] theorized: the network itself becomes an active agent shaping behavior.

7 Conclusion and Policy Implications

Why Transparency Fails

Regulations like GDPR and CCPA assume market failure comes from *information asymmetry*, and that informed users will avoid privacy-invasive platforms. Our results challenge this: the high privacy sensitivity ($\beta_{\text{priv}} = 3.14$) shows users already know the cost. The real barrier is **structural**: leaving costs you socially more than staying costs you in privacy, making informed consent useless. Transparency and consent can't fix this, as Equation 3 shows, because the constraint is network structure, not individual knowledge. Regulatory frameworks focused on disclosure are treating symptoms, not the cause.

Interoperability as a Solution

Restoring competition means decoupling the social graph from the platform. **Adversarial interoperability** through mandated open protocols lets users keep their connections when switching. This structural intervention reduces network externalities ($\beta_{\text{net}} \cdot N_{i,p}^{(\text{portable})} \approx 0$), so privacy preferences can actually influence choice. With network

portability, regulators can break the lock-in trap and shift from network-dominated monopolies to feature-driven competition, where platforms compete on privacy and service quality, not just network size. This fixes the root cause: the structural advantage from network topology that lets platforms extract behavioral surplus without competition.

Our findings show surveillance capitalism works through quantifiable mathematical relationships. The lock-in trap comes from network topology structure plus platform strategies that exploit it, not from user preferences or information gaps. Breaking it requires changing the structural incentives, going beyond transparency and consent to fix the network externalities that create monopolies. Only structural interventions can restore user agency and make privacy protection a competitive advantage instead of a cost to minimize.

References

[1] Manuel Castells. *The Rise of the Network Society*, volume 1 of *The Information Age: Economy, Society and Culture*. Wiley-Blackwell, Chichester, UK, 2nd edition, 2010.

[2] Fan R. K. Chung. *Spectral Graph Theory*, volume 92 of *CBMS Regional Conference Series in Mathematics*. American Mathematical Society, Providence, RI, 1997.

[3] Fortune Business Insights. Data privacy software market size, share & industry analysis, 2024. Accessed: 2024.

[4] Michel Foucault. *Discipline and Punish: The Birth of the Prison*. Pantheon Books, New York, 1977. Original work published 1975.

[5] Bruno Latour. *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford University Press, Oxford, 2005.

[6] Julian McAuley and Jure Leskovec. Learning to discover social circles in ego networks. In *Advances in Neural Information Processing Systems*, volume 25, 2012.

[7] George Orwell. *1984*. Secker & Warburg, London, 1949.

[8] Stanford Network Analysis Project. Social circles: Facebook, 2012. Accessed: 2024.

[9] Joseph E Stiglitz. *Economics of the Public Sector*. W. W. Norton & Company, New York, 3rd edition, 2000.

[10] Samuel D Warren and Louis D Brandeis. The right to privacy. *Harvard Law Review*, 4(5):193–220, 1890.

[11] Shoshana Zuboff. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs, New York, 2019.