Against Namespace Laundering

Flyxion

January 14, 2026

Abstract

This essay argues that the accelerating collapse of trust on contemporary digital platforms is driven by a structural failure in identity architecture that can be described as *namespace laundering*. When names, reputations, and institutional signifiers are allowed to circulate without enforced binding to persistent histories, platforms enter a high-entropy regime in which impersonation, metric manipulation, and predatory advertising become not merely possible but inevitable. The essay contends that this failure is not remediable within the incentive structures of current platforms and proposes that any viable response must treat identity as infrastructure rather than content. As a speculative extension, it explores containment-oriented design strategies for adversarial actors in systems where direct enforcement is economically disincentivized.

1 Introduction

A recurring experience on contemporary social platforms illustrates the problem this essay addresses with unusual clarity. A user receives a friend request from an account bearing the name of a well-known public figure, but the profile is incomplete: no photograph, minimal history, few visible connections. The question arises almost immediately: is this actually the person it claims to be? A few days later, a second request arrives, bearing the same name, this time adorned with a verified badge as its profile image. The ambiguity does not resolve; it compounds. The badge itself is now suspect, since it can be trivially copied, generated, or simulated. The user is left without any reliable means of adjudicating authenticity.

This experience is no longer exceptional. It is symptomatic of a deeper architectural failure in how identity is represented and enforced in large-scale digital systems. The problem is not merely that impersonation exists, but that platforms have systematically removed their own capacity to distinguish authentic identity from counterfeit appearance. This condition, which I refer to as *namespace laundering*, arises when names and reputational markers are decoupled from the histories that once gave them meaning.

Namespace laundering is not confined to interpersonal deception. The same mechanism underlies the contemporary advertising ecosystem, in which entities may claim to be legitimate businesses, medical authorities, financial experts, or mental health professionals without providing evidence of qualification, continuity, or accountability. Because platforms allow any actor to purchase reach under

any name, the symbolic economy of trust is flooded with low-cost replicas of credibility. The resulting environment is not merely unpleasant; it is structurally unsafe.

2 Identity as Infrastructure, Not Representation

In computational systems, a namespace is not a decorative feature. It is a binding structure that ensures that references remain stable across time and operations. When a name ceases to uniquely identify an object, the system does not merely become confusing; it becomes incoherent. Operations that depend on historical accumulation—such as reputation, authorization, or accountability—cease to function.

Digital platforms, however, increasingly treat identity as a mutable surface attribute rather than as infrastructural binding. Names, badges, and profile markers are presented as signals, not guarantees. Crucially, these signals are cheap to reproduce. A verified badge can be copied as an image. A familiar business name can be reused without proof. A public figure's likeness can be generated synthetically. When these markers are no longer scarce, they cease to perform their coordinating function.

This is not an accidental oversight. Platforms have systematically optimized for growth, engagement, and advertising throughput, and in doing so have weakened the constraints that once preserved identity coherence. The result is that identity becomes a non-rival good: it can be duplicated, fragmented, and repurposed without cost. Under these conditions, reputation cannot accumulate. It can only be simulated.

3 Goodhart Collapse and Advertising Saturation

The saturation of advertising in social feeds provides a particularly stark illustration of the consequences of namespace laundering. As advertising inventory expands, it begins to displace organic content, overwhelming years of deliberate curation performed by users who followed specific individuals, disciplines, and communities while actively blocking unwanted domains. This curation represented a long-term investment in semantic coherence. The advertising flood nullifies it in seconds.

More troubling than volume is content. Ads increasingly claim authority in domains where false claims carry real-world harm: financial prediction, medical advice, psychological treatment, and holistic health interventions. These claims are often presented under names or brands that imply legitimacy but lack any binding to verifiable expertise. Because platforms do not require proof of qualification or continuity, there is no structural barrier preventing the appropriation of trust-laden language.

From the platform's perspective, this is not a failure but a success. The system is performing exactly as designed. Advertising is purchased, engagement is generated, metrics improve. The fact that the underlying claims are false or dangerous is orthogonal to the optimization objective. Indeed, predatory or sensational claims often perform better under engagement-driven ranking.

This is the core of Goodhart collapse in identity systems. When optimization pressure is applied to metrics that are no longer anchored to stable referents, the system selects for imitation rather than substance. Namespace laundering becomes the dominant strategy.

4 Why the Problem Is Not Fixable In-Platform

It is tempting to believe that better moderation, improved verification, or more sophisticated machine learning could resolve these issues. This belief is mistaken. The problem is not epistemic but structural. Platforms lack both the incentive and the authority to enforce identity coherence at the scale required.

First, penalizing impersonation and fraudulent advertising directly conflicts with revenue models that monetize reach rather than legitimacy. The most egregious abuses are often the most profitable. Second, once identity has been treated as fungible for long enough, the platform no longer possesses a reliable baseline against which to judge authenticity. Enforcement becomes arbitrary, selective, and legally risky.

Most importantly, platforms cannot retroactively reconstruct identity histories that were never preserved. When names have been allowed to float free of binding constraints, there is no authoritative ledger to consult. The system has destroyed its own memory.

For this reason, proposals to "fix" existing platforms by tightening rules are largely performative. At best, they slow degradation. At worst, they provide cover for continued exploitation.

5 Containment Without Enforcement

If direct enforcement is economically and structurally infeasible, an alternative design approach suggests itself: containment rather than correction. Instead of attempting to identify and remove malicious or fraudulent actors, platforms could isolate them into environments where their behavior no longer causes harm.

One speculative model is the creation of unconnected, game-like interaction spaces in which suspected scam accounts experience the illusion of success. Within these environments, accounts receive simulated engagement, simulated responses, and simulated conversions, while being structurally disconnected from real users and real economic impact. From the perspective of the adversarial actor, the system appears functional. From the perspective of the platform's integrity, damage is minimized.

Such an approach reframes moderation as adversarial sandboxing rather than moral adjudication. It acknowledges that some classes of behavior are persistent, adaptive, and incentive-aligned, and therefore cannot be eliminated without destroying the revenue model that supports them. Containment accepts this reality and routes harmful optimization into closed loops.

While this proposal raises ethical and technical questions, it has the virtue of aligning system incentives with harm reduction rather than performative enforcement.

6 Against Namespace Laundering

The broader claim of this essay is that trust cannot survive in systems that allow namespaces to be laundered. When names, reputations, and institutional signifiers are treated as reusable tokens rather

than as bindings to history, the system enters an irreversible entropy cascade. Under such conditions, neither individual judgment nor algorithmic moderation can restore meaning.

Identity must be treated as infrastructure. This implies persistence, cost, and enforceable continuity. Without these properties, every optimization effort accelerates collapse. With them, reputation becomes possible again—not as a signal to be gamed, but as a history to be lived with.

The choice facing digital platforms is therefore not between openness and control, nor between growth and safety. It is between conserving meaning through structural constraint and continuing to launder namespaces until trust itself becomes indistinguishable from noise.

7 Cryptographic Identity and Sybil Resistance

The preceding analysis establishes that namespace laundering is not a social pathology but a structural failure: the collapse of injective identity binding under optimization pressure. Any credible response must therefore address identity at the architectural level. Cryptographic identity provides a necessary, though not sufficient, foundation for restoring namespace coherence in adversarial digital environments.

At its core, cryptographic identity replaces declarative naming with *provable continuity*. An identity is no longer defined by a mutable label but by possession of a private key that authorizes actions over time. The public key functions as a stable referent; actions signed by the corresponding private key are unambiguously attributable to the same evolving agent. This construction enforces exclusivity and continuity by design rather than by policy.

However, cryptographic identity alone does not solve the problem of impersonation at scale. While it prevents unauthorized takeover of a single identity, it does not prevent the mass creation of identities. This is the classical *Sybil problem*: when the cost of identity creation is negligible, an adversary can generate arbitrarily many identities and thereby simulate consensus, popularity, or legitimacy.

Sybil resistance is therefore not optional. It is the mechanism by which a system enforces scarcity in its namespace. Without some form of cost, friction, or coupling to scarce resources, cryptographic identities merely formalize the ambiguity they are meant to resolve.

Existing approaches to Sybil resistance illustrate the trade-offs involved. Proof-of-work imposes computational cost but is energy-intensive and poorly aligned with social systems. Proof-of-stake ties identity weight to capital, reinforcing wealth concentration. Web-of-trust models rely on existing social graphs, which are themselves vulnerable to laundering when identity is cheap. Biometric approaches introduce privacy and coercion risks. None of these mechanisms is universally adequate, but all share a critical insight: identity must be *expensive* in at least one dimension to remain meaningful.

Within the framework of namespace coherence, Sybil resistance serves a specific informational role. It bounds the identity dispersion coefficient by ensuring that the number of apparent identities cannot diverge arbitrarily from the number of actual agents. This bound is what prevents attributional entropy from overwhelming the system. The goal is not perfect uniqueness, but controlled

injectivity: a regime in which identities are sufficiently costly, persistent, and entangled with history that duplication is disincentivized.

Crucially, cryptographic identity shifts enforcement from interpretation to physics. Instead of asking whether an account is authentic, the system asks whether an action is valid under a persistent key. This eliminates entire classes of moderation problems by removing ambiguity at the substrate level. Impersonation becomes cryptographically impossible rather than socially discouraged.

Yet even in cryptographic systems, identity laundering can reappear if higher-level semantics are decoupled from cryptographic continuity. A key can be abandoned and replaced; reputation can be reset; symbols of trust can be reattached elsewhere. This demonstrates that cryptography is a necessary but insufficient condition for identity coherence. It must be integrated with mechanisms that bind history, cost, and consequence to identity over time.

From the perspective of this essay, cryptographic identity is best understood as the *base layer* of a namespace, not its entirety. It provides the invariant needed for accumulation, but it does not by itself prevent strategic fragmentation. To resist namespace laundering, cryptographic identity must be coupled to systems that preserve historical traceability across actions, artifacts, and representations. Only then does it function as infrastructure rather than ornament.

The next section will formalize these claims in information-theoretic terms and outline a concrete implementation strategy in which identity coherence is enforced through content-level traceability within an operating system and social media platform.

8 Information-Theoretic Identity, Recidivism, and Traceable Media

To understand why namespace laundering persists despite increasingly sophisticated moderation systems, we must move beyond social explanations and formalize the problem in information-theoretic terms. At its core, namespace laundering is not a failure of detection but a failure of memory. Current platforms are architecturally incapable of binding actions into a continuous informational history, and therefore incapable of recognizing recidivism as a structural phenomenon.

8.1 Identity as an Information Channel

Let X denote the true agent and Y the observed identifier (account name, page, advertiser, or profile). In a coherent identity system, the mapping $X \longrightarrow Y$ is injective, and the conditional entropy $H(X \mid Y) = 0$. Each action observed under Y can be unambiguously attributed to a single evolving history.

Namespace laundering violates this condition. When identity is cheap and resettable, the platform induces a many-to-one or many-to-many mapping between agents and identifiers. The result is *attributional entropy*: $H(X \mid Y) > 0$. Crucially, this entropy is not epistemic. It cannot be reduced by better classifiers, larger models, or more aggressive moderation. It is baked into the channel itself.

Recidivism emerges naturally in this regime. An actor who is banned, demoted, or flagged simply re-enters the system under a new identifier. Because the platform lacks a persistent binding mechanism, the past does not constrain the future. The system therefore cannot learn, cannot punish repeat

behavior, and cannot accumulate negative evidence. From an information-theoretic perspective, the platform is operating as a memoryless channel.

This explains a widely observed phenomenon: platforms may occasionally remove individual scam accounts or misleading ads, but they never meaningfully penalize the *actors* behind them. There is no concept of repeat offense because there is no stable object to which offenses can attach.

8.2 Why Current Platforms Cannot Address Recidivism

The inability to address recidivism is not an oversight; it is a direct consequence of platform incentives and architecture.

First, current platforms lack authoritative identity binding. They explicitly avoid strong identity verification because it introduces friction, legal liability, and regulatory exposure. Second, even if they wished to act, they have no internal representation of "the same actor over time" beyond weak heuristics such as IP ranges or device fingerprints, which are deliberately unreliable and legally constrained.

More importantly, recidivism is profitable. The same structural ambiguity that enables impersonation also maximizes engagement volume and advertising throughput. Scam ads, fake experts, impersonated celebrities, and synthetic businesses generate revenue regardless of their legitimacy. Penalizing repeat offenders would require tracking them across identities, which would directly conflict with the platform's growth and monetization model.

As a result, moderation is intentionally shallow. Platforms remove content, not actors. They reset state rather than accumulate consequence. The system is designed to forget.

From the perspective of this theory, this is not merely a moral failure but a physical one: entropy is continually injected into the system faster than it can be dissipated, guaranteeing collapse into noise.

8.3 Identity-Embedded Media as Structural Memory

To restore memory, identity must be bound not only to accounts but to artifacts. This motivates a design in which identity coherence is enforced at the level of content itself.

In the proposed operating system and social media platform, each identity is associated with a cryptographic hash derived from a persistent key. Every media object—image, video, audio, or document—produced by that identity is transformed through a compression or encoding pipeline that incorporates this identity hash as an invariant parameter.

Importantly, this mechanism does not rely on a visible or even conventional watermark. The identity hash is instead incorporated directly into the compression basis itself, such that the act of compression becomes identity-conditioned. For a given identity, the transformation is deterministic, ensuring that the same agent will consistently imprint the same structural signature across instances. At the same time, these signatures are statistically detectable when analyzed at scale, allowing aggregation and inference without requiring perceptual visibility.

Because the modulation operates at the level of the compression basis rather than superficial pixel features, it remains robust under common transformations such as re-encoding, cropping, resizing, and format conversion. Crucially, this approach allows compressed artifacts to be collated across platforms and over time, enabling persistent attribution even in the absence of explicit coordination between systems or the cooperation of the original platform.

The result is that artifacts carry an identity signature at the information level. Even if an image is reposted, stripped of metadata, or slightly altered, it remains probabilistically attributable to the identity that generated it. This converts media from a free-floating symbol into a traceable historical object.

From an information-theoretic standpoint, this increases the mutual information $I(X; A)$ between the agent X and the artifact A. The channel no longer destroys provenance. Recidivism becomes measurable because repeated behavior leaves correlated traces across identities, accounts, and contexts.

8.4 From Moderation to Structural Constraint

This design reframes content moderation entirely. Instead of attempting to classify intent or truth at the semantic level, the system enforces constraint at the structural level. Actors who repeatedly engage in deceptive or harmful behavior cannot shed their past by renaming themselves. Their actions remain statistically linked, even across pseudonyms.

This also enables graduated response rather than binary bans. Identities can be rate-limited, sandboxed, or diverted into isolated environments based on accumulated evidence. Your proposal of placing malicious actors into unconnected, gameified environments—where they believe they are interacting with real users but are not—is a natural extension of this logic. The system preserves external coherence while allowing adversarial energy to dissipate harmlessly.

Most importantly, this architecture makes recidivism expensive. The cost of abandoning an identity is no longer zero, because doing so also abandons accumulated reach, compression advantages, and artifact continuity. Identity becomes sticky in the only way that matters: informationally.

8.5 Why This Cannot Be Retrofitted

Finally, it must be stated plainly: this approach cannot be meaningfully retrofitted onto existing platforms. Their data models, business incentives, and legal posture are fundamentally incompatible with persistent identity coherence. They neither possess nor desire the authority required to collate behavior across time, artifacts, and pseudonyms.

Any genuine solution therefore requires new platforms and operating systems built with identity as infrastructure from the outset. Attempting to layer trust atop a system designed to erase history is futile. Once the namespace has been laundered, meaning cannot be reconstructed.

This is the core claim of *Against Namespace Laundering*: trust, reputation, and truth are not properties of content or users. They are emergent properties of constrained systems. Without memory, there is no accountability. Without accountability, there is only entropy.

9 Recidivism, Platform Amnesia, and the Economics of Forgetting

A defining characteristic of namespace laundering on contemporary platforms is the complete absence of any meaningful treatment of recidivism. While individual accounts, advertisements, or posts may be removed, downgraded, or quietly suppressed, the underlying actors responsible for repeated abuse encounter no durable constraint. The system behaves as though each incident were unprecedented. This is not a failure of enforcement capacity but a consequence of architectural amnesia.

Recidivism requires memory. To recognize a repeat offense, a system must be able to bind present actions to a persistent historical subject. Current platforms lack such a subject. Identity is fragmented into disposable tokens, and enforcement actions are applied only to the token currently visible, never to the agent producing them. Once a token is destroyed, the platform considers the problem solved. From the system's internal perspective, the offending entity has ceased to exist.

This design choice creates a perverse asymmetry. Legitimate users accumulate history, preferences, social ties, and curated environments over years or decades, while malicious or deceptive actors enjoy perfect historical reset at negligible cost. The more aggressively a platform polices individual manifestations of abuse, the more it incentivizes actors to externalize that cost by cycling identities. The platform thus converts enforcement itself into a driver of entropy.

Crucially, recidivism is not merely tolerated; it is structurally invisible. Because identity is not treated as a conserved quantity, there is no internal variable corresponding to "repeat offender." Each new account, advertiser, or page enters the system as an uncorrelated prior. Even when platforms are aware, informally, that the same behaviors recur with statistical regularity, they possess no formal mechanism to bind those events into a single accountable trajectory.

This invisibility is not accidental. Persistent identity would require the platform to acknowledge continuity across actions, which would in turn imply responsibility, escalation, and exclusion. Such escalation is incompatible with the dominant revenue model, which treats activity volume, not participant integrity, as the primary objective function. Actors who generate impressions, clicks, or ad spend remain valuable regardless of the harm they cause, provided that harm is fragmented across identifiers.

The result is a system optimized to forget. Each moderation action erases evidence rather than compounding it. Each ban purges context rather than accumulating consequence. Over time, the platform becomes a high-throughput machine for laundering behavior, in which the same deceptive patterns recur endlessly under fresh names, faces, and branding. What appears externally as incompetence or negligence is internally consistent with a system whose primary invariant is growth without memory.

From an information-theoretic standpoint, this is a catastrophic failure of conservation. The platform continually observes signals of deception, fraud, and manipulation, yet discards them instead of integrating them into a persistent model of actor behavior. Information that could reduce uncertainty about future actions is destroyed at the moment it is most valuable. The entropy of the system therefore increases monotonically, not because deception is difficult to detect, but because detection has no place to attach.

This explains why appeals to better artificial intelligence, more moderators, or improved content classification invariably fail. These interventions operate downstream of the architectural failure. They attempt to infer intent from content while the system itself refuses to acknowledge continuity of agency. No classifier, however powerful, can substitute for a missing variable. Without a stable identity substrate, recidivism is not merely hard to address; it is undefined.

The proposed alternative treats recidivism as a first-class structural phenomenon rather than a moral or behavioral one. By binding identity cryptographically and embedding that binding into the informational structure of artifacts themselves, the system acquires memory. Repeated actions no longer vanish into reset tokens but accumulate statistical weight. Patterns emerge not through surveillance of individuals, but through the conservation of informational traces.

In such a system, punishment is no longer the primary mechanism of control. Constraint replaces enforcement. Actors who persistently attempt to deceive find their actions increasingly confined, redirected, or rendered ineffective, not by discretionary judgment but by structural incompatibility with the system's invariants. Recidivism ceases to be a policy problem and becomes a thermodynamic one: repeated entropy injection is damped by design.

The failure of existing platforms to address recidivism should therefore not be understood as a temporary shortcoming or a fixable oversight. It is the inevitable outcome of systems built to maximize participation while minimizing obligation. Any platform that refuses to bind actions to enduring histories cannot, by definition, learn from experience. It can only react, forget, and repeat.

In this light, the proliferation of impersonation, scam advertising, synthetic expertise, and identity abuse is not a deviation from platform logic but its purest expression. Where identity is optional, history is irrelevant. Where history is irrelevant, trust cannot accumulate. And where trust cannot accumulate, meaning itself becomes transient, performative, and disposable.

The claim is not simply that impersonation and fraud are harmful, but that platforms which structurally forget who acts undermine their own governability. By permitting identity to reset without consequence, these systems eliminate the informational substrate necessary for accountability, adaptation, and institutional stability. Moderation applied after the fact cannot restore this substrate. Only architectures that conserve history can sustain governance.

10 Conclusion: Against Namespace Laundering

This essay has argued that the contemporary crisis of trust on digital platforms is neither accidental nor primarily cultural, but architectural. The proliferation of impersonation, scam advertising, synthetic authority, and recidivist abuse is not a failure of moderation, intelligence, or goodwill. It is the predictable consequence of systems that treat identity as a disposable label rather than as a conserved structural primitive. Namespace laundering is not an exploit at the margins of these platforms; it is a dominant equilibrium produced by their core design choices.

By reframing identity as namespace infrastructure, the analysis has shown that trust, reputation, and meaning are not subjective overlays that can be optimized after the fact, but informational quantities that require stable binding to persist over time. When actions cannot be uniquely and persistently

associated with histories, attribution collapses, metrics decouple from substance, and optimization pressure inevitably selects for imitation over contribution. Goodhart collapse, metric farming, and performative engagement follow not because actors are irrational, but because the system makes authenticity strictly more expensive than deception.

The essay has further demonstrated that this collapse is thermodynamic rather than linear. Using the RSVP framework, platform dynamics were shown to undergo phase transitions when identity dispersion exceeds a critical threshold. Beyond this point, coherence does not degrade gradually but bifurcates into a high-entropy regime characterized by vector churn and reputational dissipation. The presence of hysteresis explains why mature platforms cannot easily recover trust once it has been lost: the scalar basins that once stabilized meaning have been flattened, and restoring them requires forces far greater than those originally needed to maintain them.

Current platform responses—account bans, content removal, AI moderation, and policy adjustments—fail because they operate downstream of this collapse. They act on manifestations rather than causes. Most critically, they do nothing to address recidivism. By allowing offenders to re-enter the system under fresh identifiers at negligible cost, platforms systematically erase the very information required to learn, escalate, or deter. Enforcement becomes a form of entropy production, accelerating the loss of meaning rather than conserving it.

Against this backdrop, the proposed alternatives are deliberately architectural rather than punitive. Cryptographic identity, Sybil resistance, and information-theoretic binding mechanisms are not offered as tools of surveillance or control, but as means of restoring conservation laws. By hashing identities, embedding those hashes into shared artifacts, and ensuring that variations remain contractibly bound to a single historical trajectory, a system can acquire memory without sacrificing pseudonymity. In such a system, recidivism becomes structurally visible, manipulation becomes increasingly costly, and deception is constrained not by judgment but by incompatibility with the system's invariants.

The speculative proposal of isolating deceptive actors within unproductive, game-like environments underscores this shift in perspective. Rather than attempting to morally reform or continuously police bad behavior, the system can simply deny it informational leverage. When identity is conserved and consequences accumulate, abuse ceases to scale. When identity is laundered, no amount of intelligence can prevent collapse.

The broader implication is that many existing platforms may be beyond repair. Their economic incentives are aligned with identity fragmentation, and their architectures lack the authority to collate behavior across time. In such cases, recovery may be impossible without abandoning the system itself. New platforms must therefore be built alongside the old, grounded in constraint-first design, offering continuity through trust transfer rather than restoration.

Ultimately, this essay has advanced a single, unifying claim: meaning is not generated by optimization, but preserved by constraint. Identity coherence is not a feature to be balanced against growth or engagement; it is the precondition for any system that claims to support knowledge, reputation, or social reality. Against namespace laundering is thus an argument for remembering—architecturally, informationally, and irrevocably—who acts in the world. Only systems that remember can govern.

References

[1] C. A. E. Goodhart. Problems of monetary management: The U.K. experience. In *Papers in Monetary Economics*, Reserve Bank of Australia, 1975.

[2] D. T. Campbell. Assessing the impact of planned social change. *Evaluation and Program Planning*, 2(1):67–90, 1979.

[3] M. Strathern. *"Improving Ratings": Audit in the British University System. European Review*, 5(3):305–321, 1997.

[4] J. Z. Muller. *The Tyranny of Metrics.* Princeton University Press, Princeton, 2018.

[5] E. M. Bender, T. Gebru, A. McMillan-Major, and S. Shmitchell. On the dangers of stochastic parrots: Can language models be too big? In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, 2021.

[6] C. Olah et al. The building blocks of interpretability. *Distill*, 3(3), 2018.

[7] K. Friston. The free-energy principle: A unified brain theory? *Nature Reviews Neuroscience*, 11(2):127–138, 2010.

[8] R. Landauer. Irreversibility and heat generation in the computing process. *IBM Journal of Research and Development*, 5(3):183–191, 1961.

[9] C. E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 623–656, 1948.

[10] H. R. Varian. Market structure in the network age. *Journal of Economic Perspectives*, 33(3):91–110, 2019.

[11] C. Doctorow. The enshittification of TikTok. *Pluralistic*, 2023.

[12] S. Zuboff. *The Age of Surveillance Capitalism.* PublicAffairs, New York, 2019.

[13] L. Lamport. The part-time parliament. *ACM Transactions on Computer Systems*, 16(2):133–169, 1998.

[14] S. Mac Lane. *Categories for the Working Mathematician.* Springer, New York, 2nd edition, 1998.

[15] R. Ghrist. *Elementary Applied Topology.* Createspace, 2014.

[16] J. C. Scott. *Seeing Like a State.* Yale University Press, New Haven, 1998.

[17] L. Lessig. *Code and Other Laws of Cyberspace.* Basic Books, New York, 1999.