# A Taxonomy of Collusion in Information Systems

Kevin Armbruster
Technical University of Munich, CHN
kevin.armbruster@tum.de

Niclas Kannengießer
Karlsruhe Institute of Technology
niclas.kannengiesser@kit.edu

Mikael Beyene
Karlsruhe Institute of Technology
mikael.beyene@kit.edu

Gabriela Ciolacu
Karlsruhe Institute of Technology
gabriela.ciolacu@kit.edu

Ali Sunyaev
Technical University of Munich, CHN
sunyaev@tum.de

## Abstract

*Collusion poses a pervasive threat to information systems (IS), undermining fairness, trust, and system integrity. Existing research, however, often focuses narrowly on specific cases or emphasizes either social or technical aspects, resulting in fragmented insights and limited generalizability. This narrow scope hampers the development of broadly effective protection strategies. Recognizing collusion as a sociotechnical phenomenon shaped by the interplay between social actors and technical artifacts, we developed a case-agnostic taxonomy that helps uncover and classify various forms of collusion in IS. Using an iterative approach, we synthesized insights from multidisciplinary academic literature and descriptive legal cases. Grounded in general systems theory, the taxonomy offers a robust structural foundation for analyzing collusion in IS. This taxonomy benefits practice by capturing the structural characteristics of collusion, enabling more systematic analysis, detection, and mitigation.*

**Keywords:** antitrust, collusion, cybersecurity, sociotechnical systems, taxonomy.

## 1. Introduction

When ride-hailing drivers coordinate logoffs via online forums, the resulting artificial drop in driver supply prompts the pricing algorithm to increase customer fares (Bai et al., 2023). This behavior is a form of collusion—broadly referring to social actors and/or technical artifacts that covertly agree to work together to gain benefits or harm other actors (Ciccarelli & Lo Cigno, 2011).

Collusion is a persistent issue in information systems (IS), threatening systems like online marketplaces and peer-to-peer networks, where it harms honest actors, such as customers and competitors, and undermines the integrity of the system itself. In economic markets, for example, collusion can undermine competition, diminish product quality, and stifle innovation (Villamil et al., 2024). Similarly, in peer-to-peer networks, colluders might exploit resources (e.g., bandwidth and storage) or undermine system mechanisms (e.g., auditing and voting), leading to poor decisions and unchecked misbehavior (Ciccarelli & Lo Cigno, 2011). Thus, collusion fosters unfair conditions by facilitating advantages for collusive actors while leaving honest actors at a disadvantage.

Collusion in IS is a sociotechnical issue that emerges from the interplay of social actors and the technical artifacts they use. Such actors leverage and are constrained by technical artifacts to achieve collusive goals. The technical artifacts not only enable but also shape collusive behavior, for example, by influencing how ride-hailing drivers coordinate logging off an app in a particular zone to trigger surge pricing. The social and technical elements are not merely coexistent—they are deeply entangled.

Although collusion could occur within most IS, existing research predominantly concentrates on collusion in specific cases. These cases are predominantly analyzed with a focus on technology (e.g., peer-to-peer systems, blockchain technology, and machine learning; Ciccarelli & Lo Cigno, 2011; Schwalbe, 2019; Wu et al., 2018) or social aspects (e.g., auctioning, organizational, and gaming; Laasonen et al., 2011; Laffont & Martimort, 1998; Villamil et al., 2024) involved in collusion. This narrow, case-specific focus helps uncover different forms of collusion, but fails to capture the possible structures of collusion in IS in general. Although attempts have been made to

URI: https://hdl.handle.net/10125/112075
978-0-9981331-9-5

conceptualize the structure of collusion (e.g., Ciccarelli & Lo Cigno, 2011; Laasonen et al., 2011), developed concepts remain tied to specific contexts. The resulting lack of clarity about possible structures of collusion hinders the detection and mitigation of collusion in IS and the design of broadly applicable protection mechanisms and policies.

Because collusion transcends individual technologies and cases, a more generalized, sociotechnical concept is needed to support collusion protection of diverse IS. We therefore ask the following research question: *What are the structural dimensions and characteristics of collusion in information systems?*

We iteratively developed a collusion taxonomy that presents the structural dimensions and characteristics of collusion by alternating between the *conceptual-to-empirical* and *empirical-to-conceptual approaches* (Nickerson et al., 2013). To initiate the conceptual-to-empirical phase, we conducted a systematic literature search (Webster & Watson, 2002) to identify academic publications that present conceptualizations of collusion. Given the high number of results, we clustered the publications into thematic communities representing the main research areas related to collusion. For the empirical-to-conceptual approach, we supplemented the literature with legal cases for their rich descriptive accounts.

Our main contributions are threefold. *First*, we propose a taxonomy that describes the structure of collusion in IS agnostic of specific cases, supporting the detection and comparison of different forms of collusion—also in terms of the types of IS in which they occur. *Second*, by clarifying the key dimensions and characteristics of collusion structures, the taxonomy provides practical value to system designers, security analysts, and policymakers, enabling them to anticipate collusion beyond familiar scenarios. *Third*, the taxonomy advances theory by providing a structural foundation for analyzing collusion in IS, showing how different sociotechnical arrangements can represent equifinal pathways to successful collusion.

## 2. Background

Collusion occurs in many types of systems, including economic, political, and technical ones (Ciccarelli & Lo Cigno, 2011; Kofman & Lawarrée, 1993; Villamil et al., 2024), all of which share features with IS, such as social interactions, power structures, and technical artifacts. These shared aspects make collusion in IS a complex and multifaceted phenomenon. We draw on insights from related systems to provide context for the taxonomy developed in this work.

### 2.1. Collusion in Information Systems

We adopt the conceptualization of information systems proposed by Chatterjee et al. (2021) as our analytical lens. This conceptualization helps us analyze the interplay between social actors and technical artifacts, which is central to collusion within IS. According to this model, IS are dynamic sociotechnical systems in which social and technical subsystems co-evolve to realize the system's purposes. The social subsystem consists of social actors (e.g., individuals, groups, and organizational arrangements), while the technical subsystem encompasses technical artifacts (e.g., hardware, software, and data infrastructures). At the core of their interaction is information, its representation, flow, and transformation, through which the subsystems mutually shape each other's design and behavior in ways that support or undermine IS purposes. This coupling can be described as an affording–constraining relationship, which we refer to as a relation between social actors and technical artifacts that simultaneously enables and restricts courses of action. IS are inherently multifinal, since multiple actors can pursue different, and often conflicting, objectives within the same system. IS are also equifinal, as the same objective can be achieved through multiple technological and organizational pathways. Multifinality can allow actors to pursue their own goals, while equifinality implies that such goals may be achieved in more than one way. These properties render the affording–constraining relationship central for understanding how sociotechnical action unfolds (see Figure 1). We consider this relationship *functional* when it channels action toward the intended IS purpose and *dysfunctional* when it subverts the IS purpose.

Collusion is a dysfunctional affording–constraining relationship. We define collusion as covert cooperation among social actors and/or technical artifacts to gain unfair advantages or harm other actors (Bajari & Summers, 2002; Ciccarelli & Lo Cigno, 2011; Ezrachi & Stucke, 2016; Kerr & Cohen, 2011). We refer to collusive actors and collusive artifacts as *colluders* in the following. Collusion affords sociotechnical couplings and coordinated action that evades rules while the IS fails to impose constraints. Collusion may be enacted through social coordination mediated by technical artifacts, through algorithmic interactions that stabilize manipulative outcomes, or through hybrid constellations where social actors and technical artifacts jointly conspire. Information is the enabling medium, whether in the form of private information (e.g., insider trading) or synchronized use of public information (e.g., tacit collusion; Ezrachi & Stucke, 2016).

Where constraints are absent, weak, or misaligned, the affording–constraining relationship becomes permissive of collusion. Once collusion is initiated, collusive entities exploit both social and technical affordances. Social affordances can derive from weak monitoring, fragmented accountability, or limited sanctioning capacity. Technical affordances include low-cost communication, automation, and data access.

Because IS are equifinal, collusion can be organized through a variety of arrangements among actors and technical artifacts. These arrangements can strongly differ in their structure (e.g., number of entities involved and their interaction topology). Such structural characteristics determine how collusion is coordinated, how information is exchanged, and how advantages are secured. Understanding these structural properties is essential for explaining how different forms of coordination can converge on the same goal of successful collusion. The taxonomy presented in this work captures such structural features and provides a foundation for analyzing the multiple pathways through which collusion is performed in IS.

## 2.2. Classifications of Collusive Behavior

Several studies have conceptualized collusion in domains like computer science, economics, and politics, highlighting aspects, such as incentives, group dynamics, and governance, that are transferable to IS. Most existing research narrowly examines specific collusion cases, often through a *social* or *technical* lens, which has led to a fragmented understanding. *Social-focused* research has concentrated on the interpersonal dynamics, communication strategies, and motivations of actors (e.g., Laasonen et al., 2011; Laffont & Martimort, 1998; Villamil et al., 2024). Such studies often treat technology as either a negligible enabler or not at all. For example, analyses of bidding networks in procurement markets treat technical artifacts as mere data sources, overlooking the role of their design (Villamil et al., 2024).

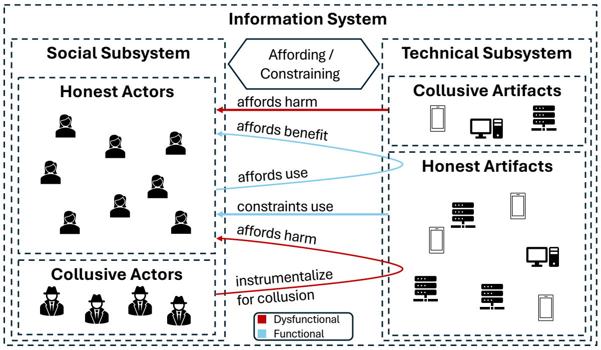

**Figure 1. Simplified conceptualization of collusion in IS. Functional relationships support intended IS purposes. Dysfunctional relationships enable the exploitation of affordances and failed constraints.**

*Technology-focused* research has primarily focused on threat models and potential attack vectors within specific technical systems, such as peer-to-peer systems, blockchain systems, and machine learning applications (e.g., Ciccarelli & Lo Cigno, 2011; Schwalbe, 2019; Wu et al., 2018). While these studies aim to detect and mitigate collusion by closing technical vulnerabilities, their scope is often confined to narrow technological boundaries. For example, peer-to-peer systems may address reputation attacks or collusive chains (Ciccarelli & Lo Cigno, 2011), but overlook social factors like coercion. Such solutions may be technically sound yet fragile when faced with real-world social dynamics.

Despite valuable contributions, the narrow focus of existing works has led to a fragmented body of specialized studies. Without an integrative concept, collusion in IS that arises from the interaction of social and technical aspects risks being overlooked. To address this issue, we developed a case-agnostic conceptual foundation that describes collusion structures in IS.

# 3. Methods

We developed a collusion taxonomy (Nickerson et al., 2013) using academic publications and legal cases.

## 3.1. Literature Search

To prepare for the taxonomy development, we conducted two targeted literature searches. The first literature search provided academic publications that describe collusion concepts useful for the conceptual-to-empirical approach. Second, we sourced descriptive legal cases, which served as empirical data for the empirical-to-conceptual approach.

**3.1.1. Literature Search for the Conceptual-to-Empirical Approach** To identify relevant academic publications presenting collusion concepts, we first conducted a systematic literature search (Webster & Watson, 2002). The large number of results prompted us to group publications into thematic clusters to focus our analysis without sacrificing broad thematic coverage.

**Collection of Potentially Relevant Publications** We developed the search string: *(collu*) AND (strateg* OR behavio* OR characteristic* OR attack* OR* *agreement* OR formation*)*. We applied it to titles, keywords, and abstracts of English-language publications in the Web of Science database. Web of Science was selected for its broad disciplinary coverage, which enabled us to capture diverse perspectives on collusion. The search yielded 5,244 potentially relevant publications. To refine this set, we applied the inclusion criteria *English language*, *topic fit*, *uniqueness*, and *outlet ranking* (see Table 1). We removed 1,280 publications due to insufficient topic fit and excluded nine duplicates, retaining only the most recent versions. We then applied a quality filter, keeping only publications in Q1-ranked outlets according to the Scimago Journal Ranking. After filtering, 2,680 publications remained for community detection.

**Thematic Community Detection** We applied community detection to cluster the publications into thematic groups to randomly sample publications from each group during the taxonomy development while maintaining broad coverage of research perspectives. We first enriched the keyword data by concatenating the keywords from authors and Web of Science for each publication. We then removed special characters and numbers and lemmatized and lowercased terms. We also consolidated various forms of 'peer-to-peer'.

Using the Python NetworkX library (Hagberg et al., 2008), we constructed a keyword co-occurrence network—where nodes represent publications and edges are weighted by the number of shared keywords—and then applied the Louvain algorithm to detect thematic communities. To ensure robust results, we executed it 100 times with different random seeds and selected the most frequent partition. To improve community distinctiveness and robustness, we iteratively removed the most frequent, overly broad terms: 'collus', 'collus attack', 'secur', and 'experi'. After eliminating these four terms, the process yielded 12 distinct communities with a modularity score of 0.577, indicating a strong community structure.

We qualitatively validated the 12 communities based on our domain knowledge of collusion, confirming they represent distinct research themes (see Table 2). This validation prepared the publication set for the subsequent representative sampling.

**Table 1. Overview of Inclusion Criteria.**

| Name | Description |
|---|---|
| English Language | The publication must be in English. |
| Topic Fit | The publication must discuss collusion. |
| Uniqueness | Only the most recent version of the publication is included. |
| Publication Ranking | The publication must appear in a Q1-ranked outlet (Scimago Journal Ranking). |

**3.1.2. Literature Search for the Empirical-to-Conceptual Approach** For the empirical-to-conceptual approach, we compiled a second set of publications of 66 finalized legal cases. Our search strategy combined querying official legal databases—specifically the European Commission's (EC) Competition Cases Database[1] and the U.S. Department of Justice's (DoJ) Antitrust Case Filings database[2]—supplemented by case references from academic literature. The EC database search was filtered by policy area ('Antitrust & Cartels') and legal basis (Article 101 TFEU). To be included, each legal case ruling had to be a finalized judgment providing sufficient detail on how the collusion was enacted.

**Table 2. Identified Thematic Communities.**

| Community Name | Size | Top 5 Keywords* |
|---|---|---|
| Market Competition | 290 | competiti, tacit collus, oligopoli, cartel, market power |
| Trust & Fraud Detection | 94 | trust, reput, social network, fraud detect, reput system |
| Blockchain & Smart Contracts | 103 | blockchain, smart contract, evolutionari game, privaci protect, crowdsourc |
| Game Theory & Pricing | 92 | game theori, price, price competit, retail, suppli chain manag |
| Privacy-Preserving Computing | 153 | privaci preserv, privaci, server, feder learn, cryptographi |
| Online Identity Verification | 5 | sybil attack, onlin social network, spam, user behavior, measur |
| Wireless Network Security | 118 | physic layer secur, wireless communic, collud eavesdropp, stochast geometri, ad hoc network |
| Digital Content Protection | 100 | collus resist, traitor trace, fingerprint, watermark, broadcast encrypt |
| Cloud Computing Security | 104 | cloud comput, access control, attribut base encrypt, encrypt, data share |
| Repeated Games & Cooperation | 137 | repeat game, cooper, mechan design, communic, laboratori experi |
| Corruption & Governance | 138 | corrupt, china, corpor govern, gender, construct industri |
| Antitrust Enforcement | 3 | antitrust enforc, cartel organ, econom activ, trade associ, us antitrust system |

*sorted by decreasing number of occurrences

[1] https://competition-cases.ec.europa.eu/search

[2] https://www.justice.gov/atr/antitrust-case-filings

### 3.2. Taxonomy Development

We developed the collusion taxonomy following Nickerson et al. (2013). Given the equifinality of IS, dysfunctional affording–constraining relationships can take multiple forms (see Section 2.1), which informed our meta-characteristic, structure of collusive groups, and six ending conditions (Table 3). We alternated between two complementary approaches. In the *conceptual-to-empirical* approach, we randomly sampled publications from the 12 thematic communities. The sampled publications were retained only if they had a conceptual focus (e.g., conceptualizations of collusion characteristics or threat models). We repeated the process until we reached a sufficient number of conceptual publications that met our inclusion criteria. We then analyzed these publications to identify and refine dimensions and characteristics. In the *empirical-to-conceptual* approach, we examined legal cases to validate, refine, and extend the taxonomy. Two coders from the author team conducted the analysis in multiple rounds. After each round, we held discussions to resolve inconsistencies and ensure that the coding was exhaustive, mutually exclusive, relevant, representative, and concise (see Table 3).

**First Round (Conceptual-to-Empirical)** We employed a conceptual-to-empirical approach to build an initial taxonomy grounded in existing research. We used five conceptual publications from each of the 12 thematic communities, except for one community, which contained only three publications. This yielded a set of 58 publications for the qualitative analysis in this iteration. We iteratively refined codes by combining or splitting them to form distinct dimensions and characteristics. We resolved minor conflicts in the coding results between the two coders in discussions within the author team with unanimous agreement. This stage resulted in a preliminary taxonomy that contained 26 dimensions and 61 characteristics.

**Second Round (Empirical-to-Conceptual)** We refined the taxonomy using the collected legal case ruling set. We coded 17 legal cases, mapping the descriptions to the existing structure and adjusting dimensions and characteristics in team discussions. We resolved minor conflicts in the coding results as in the previous iteration. This process stopped after three cases that led to no additional changes, resulting in a more robust taxonomy of 19 dimensions and 40 characteristics, better aligned with collusion behaviors observed in practice.

**Third Round (Conceptual-to-Empirical)** We sampled one additional conceptual publication for each of the remaining communities, resulting in the analysis of 10 publications. Because the analysis yielded no changes, we deemed the taxonomy sufficiently robust. As we met all ending conditions in this iteration (see Table 3), we concluded the development process. This grounds the final taxonomy in the total analysis of 68 academic publications and 17 legal cases.

Last, we grouped the dimensions into categories to enhance the usability of the collusion taxonomy.

## 4. Collusion Taxonomy

Table 4 presents the collusion taxonomy (five categories, 19 dimensions, 40 characteristics) and illustrates its application based on eight legal cases.

### 4.1. Behavioral Dynamics

The category **behavioral dynamics** characterizes the operative behavior of colluders, focusing on the actions performed toward collusive advantage by exploiting sociotechnical affordances for coordination.

The dimension **action similarity** specifies whether colluders perform the same or different actions. This can be either *identical*, where all colluders perform the same type of action, or *distinct*, where they perform complementary actions.

The dimension **action timing** refers to the time-dependent synchronization of these behaviors, classified as either *synchronous*, executed in a

**Table 3. Objective and Subjective Ending Conditions**

| Type | Characteristics | Definition |
|---|---|---|
| Objective | Exhaustiveness | The characteristics and dimensions collectively exhaustively describe forms of collusion. |
| | Mutual exclusiveness | Characteristics (and dimensions) do not semantically overlap. |
| | Relevance | Each characteristic of each dimension is at least used once to classify a collusion in the taxonomy. |
| | Representativeness | A selection of publications from all thematic communities were incorporated into the taxonomy. |
| | Robustness | No changes (i.e., addition, merger, and split) were made to the taxonomy in the last iteration. |
| Subjective | Conciseness | The taxonomy includes a limited number of relevant dimensions and characteristics to describe the structure of collusive behavior. |

**Table 4. Classification of Exemplary Legal Cases into the Taxonomy**

| Category | Dimension | Characteristic | **RealPage**<br>(U.S. DoJ, 2025) | **Microsoft**<br>(U.S. DoJ, 2007) | **PowerCables**<br>(EC, 2014) | **Yen Interest Derivatives**<br>(EC, 2021) | **American Airlines**<br>(U.S. DoJ, 2004) | **Interbrew + Alken Maes**<br>(EC, 2001) | **Carbon & Graphite**<br>(EC, 2004) | **Activision Blizzard**<br>(U.S. DoJ, 2023) |
|---|---|---|---|---|---|---|---|---|---|---|
| Behavioral Dynamics | Action Similarity | Distinct | X | X |  | X | X |  |  | X |
|  |  | Identical |  |  | X |  |  | X | X |  |
|  | Action Timing | Asynchronous | X | X |  |  |  |  |  |  |
|  |  | Synchronous |  |  | X | X | X | X | X | X |
|  | Interaction Disposition | Competitive |  | X | X |  |  |  |  |  |
|  |  | Supportive | X |  |  | X | X | X | X | X |
|  | Interaction Modality | Collaborative |  | X | X | X | X | X | X |  |
|  |  | Cooperative | X |  |  |  |  |  |  | X |
|  | Source of Advantage | Action-based |  | X | X |  |  | X | X | X |
|  |  | Information-based | X |  |  | X | X |  |  |  |
| Composition Structure | Integration | Contained |  |  |  |  |  |  |  | X |
|  |  | Integrated | X | X | X | X | X | X | X |  |
|  | Interaction Structure | Clustered Network |  |  | X |  |  |  |  |  |
|  |  | Dense Mesh Network |  |  |  |  |  |  | X |  |
|  |  | Fully Connected Network |  |  |  |  | X | X |  |  |
|  |  | Hub-and-Spoke Network | X | X |  | X |  |  |  | X |
|  | Membership Structure | Closed |  |  |  |  | X | X | X | X |
|  |  | Open | X | X | X | X |  |  |  |  |
|  | Structural Redundancy | Redundant |  |  | X |  |  |  |  |  |
|  |  | Singular | X | X |  | X | X | X | X | X |
| Governance | Agreement Mode | Explicit |  | X | X | X |  | X | X | X |
|  |  | Tacit | X |  |  |  | X |  |  |  |
|  | Control Mechanism | Authority-based |  |  | X |  |  | X |  |  |
|  |  | Incentive-based | X | X |  | X | X |  | X | X |
|  | Decision Authority Distribution | Centralized | X | X |  |  |  | X | X | X |
|  |  | Decentralized |  |  | X | X | X |  |  |  |
|  | Enforcement Strength | Strong |  | X | X |  | X | X | X | X |
|  |  | Weak | X |  |  | X |  |  |  |  |
|  | Locus of Coordination | Social |  | X | X | X | X | X | X | X |
|  |  | Technical | X |  |  |  |  |  |  |  |
| Intent | Impact Domain | Horizontal | X |  | X |  | X | X | X | X |
|  |  | Vertical |  | X |  | X |  |  |  |  |
|  | Operational Horizon | Terminal |  |  |  | X |  |  |  |  |
|  |  | Standing | X | X | X |  | X | X | X | X |
|  | Reward Distribution | Collective |  |  | X |  |  |  |  |  |
|  |  | Individual | X | X |  | X | X | X | X | X |
| Resources | Investment | Cost-Bearing | X | X |  |  |  |  | X |  |
|  |  | Cost-Free |  |  | X | X | X | X |  | X |
|  | Resource Variety | Heterogeneous | X | X |  | X | X |  | X | X |
|  |  | Homogeneous |  |  | X |  |  | X |  |  |

coordinated temporal pattern, or *asynchronous*, occurring without a specific sequence.

The dimension **interaction disposition** captures the internal relationship of colluders. This can be *supportive*, where colluders assist one another to ensure collective success, or *competitive*, where an underlying rivalry persists. In a competitive disposition, colluders cooperate against external entities but simultaneously compete for individual advantage within the group, such as a larger share of profits or a more favorable position.

The dimension **interaction modality** distinguishes how colluders work together. A *cooperative* modality involves colluders working independently toward a shared goal; their individual actions are parallel, and success depends on the sum of these contributions rather than their direct integration during execution. In contrast, a *collaborative* modality involves colluders working interdependently. Tasks are intertwined and the success of one colluder's action is directly contingent on the action of another, often requiring a coordinated sequence of actions to achieve the desired effect.

The dimension **source of advantage** specifies the primary medium that drives the collusive advantage. In *action-based* collusion, the advantage arises directly from the synchronization of behaviors, often relying on public information. In *information-based* collusion, the advantage stems from exclusive control over private information, which is strategically shared, withheld, or manipulated to create information asymmetries.

## 4.2. Composition Structure

**Composition structure** describes the organizational and relational attributes in a collusive group.

The dimension **integration** describes the degree to which the collusive group is embedded within the larger system in which it operates. A group can be *integrated*, meaning it is well-connected and functions as a part of the broader system, frequently interacting with non-colluding entities. Such interactions may be necessary to execute the collusion or to mask its activities within normal operational patterns. In contrast, a *contained* group operates in relative isolation. This self-contained structure can serve to reduce the risk of detection or may simply reflect a collusive goal that does not require external engagement.

The dimension **interaction structure** describes the network topology formed by the interactions between colluders. At the most connected end of the spectrum is the *fully connected network*, where every colluder is linked to all others, creating a completely integrated group. A slightly less connected variant is the *dense mesh network*, where most colluders are connected, but not all. *Hub-and-spoke networks* involve a central entity that intermediates interactions between peripheral colluders. A *clustered network* is composed of distinct subgroups that are tightly connected internally but only loosely connected to other clusters.

The dimension **membership structure** addresses the consistency of the collusive group's membership over time. A group can be *closed*, characterized by a fixed and unchanging set of colluders. This often implies high barriers to entry and a stable, long-term arrangement among the colluders. In contrast, an *open* group exhibits a composition, where colluders may join or leave the arrangement over its lifespan. This can be a deliberate feature of collusion, designed for flexibility, or a natural consequence of a low-commitment structure where colluders can easily enter and exit.

The dimension **structural redundancy** describes the arrangement and distribution of critical capabilities within the collusive group. A structure is considered *singular* when it consolidates essential functions or resources within an irreplaceable minority of its colluders. This concentration creates a single point of failure, making the entire collusion vulnerable to the disruption or removal of these key colluders. Conversely, a structure is *redundant* when critical capabilities are distributed across multiple colluders. This ensures that the loss of one or more colluders does not necessarily compromise the group's ability to function, thereby increasing its overall resilience.

## 4.3. Governance

The category **governance** refers to the internal management and control systems of a collusive group, reflecting the internal affording and constraining relationships that afford coordinated action while constraining individual defection.

The dimension **agreement mode** refers to how colluders align their actions. This can be *explicit*, where coordination is achieved via direct communication such as meetings, phone calls, or online forums. In contrast, *tacit* collusion emerges as colluders align their behavior by mutually observing and inferring a shared strategy.

The dimension **control mechanism** describes the primary method used to ensure a high degree of compliance within the collusive group. It can be *authority-based*, where adherence is achieved through commands issued by a recognized leader or a formal governing structure, relying on hierarchy and obedience. Alternatively, the mechanism can be *incentive-based*, which enforces compliance through a system of explicit rewards for cooperation or penalties for defection.

**Decision authority distribution** describes the distribution of power to make key decisions within the collusive group. In a *centralized* structure, a single entity or a small, dominant subgroup makes all key decisions. Conversely, decision-making power is more evenly distributed in *decentralized* structures, enabling all colluders to participate equitably and autonomously in key decisions, often through consensus.

The dimension **enforcement strength** describes the degree to which the collusive group can ensure adherence to its agreed-upon actions, particularly in the face of individual incentives to defect. Enforcement is considered *weak* when the arrangement relies primarily on continuous mutual benefit to ensure compliance. In such cases, colluders can withdraw from the agreement without facing significant group-imposed consequences, making the collusion stable only as long as cooperation remains individually advantageous for all colluders. In contrast, enforcement is *strong* when the collusion is maintained through credible deterrents, such as coercion or severe penalties, which sustain the arrangement even if it goes against a colluder's immediate interests.

The dimension **locus of coordination** refers to the primary agent responsible for orchestrating the collusive activities. A *social* locus of coordination is driven by direct interaction and decision-making of social actors, such as agreements made through meetings or secure messaging. Conversely, technical artifacts facilitate collusion with a *technical* locus of coordination. For example, algorithms execute coordinated actions based on learned behavior and real-time data inputs, without human intervention at the moment of execution.

### 4.4. Intent

The category **intent** encapsulates the strategic purpose and outcomes of a collusion.

The dimension **impact domain** describes the scope of the collusion's effect within a system. A *horizontal* impact is confined to a single, shared functional area. This typically involves collusion between peer colluders performing similar roles, such as multiple user accounts coordinating to manipulate a content rating or voting system. In contrast, a *vertical* impact spans multiple, often sequential, processes or components of the system. This form of collusion involves colluders with distinct and complementary roles coordinating their actions across different stages of a workflow, such as one user creating fraudulent data and another using a separate system function to exploit it.

The dimension **operational horizon** describes the intended continuity of the collusive activity. Collusion can be *terminal*, meaning it is formed for a specific objective and is typically dissolved once that goal is achieved. In contrast, *standing* collusion is an ongoing arrangement established for long-term operation to maintain strategic advantages.

The dimension **reward distribution** describes the method by which gains from the collusion are distributed among its colluders. The method can be *individual*, where each colluder directly earns and retains their own reward based on their specific actions within the collusion. In contrast, a *collective* method involves a process where rewards are distributed among colluders according to a pre-arranged scheme. This can range from pooling all monetary gains for splitting to arrangements, where colluders take turns winning contracts.

### 4.5. Resources

The category **resources** pertains to the assets and investments that enable and sustain a collusive group.

The dimension **investment** describes whether there is a significant cost associated with the formation or execution of a collusion. An arrangement is considered *cost-bearing* when performing the collusive behavior requires an expense of resources, such as financial payments or a significant investment of time. In contrast, collusion is *cost-free* when the required action can be performed with negligible expense, often because it involves simple adjustments to normal activities or leverages pre-existing capabilities.

The dimension **resource variety** describes the diversity of the resources available among colluders. Resources are *homogeneous* when all colluders possess similar assets and capabilities. Conversely, resources are *heterogeneous* when colluders bring dissimilar but complementary assets to the group, creating a synergistic effect where different roles are essential to the collusion's success.

## 5. Discussion

The taxonomy and its development led us to several key findings discussed in this section. Moreover, this section explains this work's key contributions, its limitations, and outlines future research directions.

### 5.1. Principal Findings

Collusion in IS spans a wide array of technologies, architectures, and application domains. Our analysis of 12 thematic communities of publications revealed diverse research foci, from traditional economics to computer science fields on blockchain, privacy-preserving computing, and security of wireless networks. This diversity suggests that no IS is inherently immune to collusion. Collusion can adapt to contexts and evade simple detection. Research has a strong focus on how specific technologies can mitigate collusion, especially in areas like blockchain technology and cloud computing.

The taxonomy indicates that the complexity and variability of collusion make it difficult to capture all possible interaction patterns. Collusion does not necessarily correspond to a static pattern but a dynamic sociotechnical strategy that adapts to context. As such, robust detection and mitigation call for a nuanced, structural understanding of manifold behaviors of collusive groups, as offered in this study.

Literature highlights a paradigm shift: technology itself can act collusively (Ezrachi & Stucke, 2016). Social actors are no longer the sole drivers of collusion; they increasingly outsource these behaviors to algorithms, whether intentionally or unintentionally. Practices, such as algorithmic pricing where competing systems adjust prices based on each other's outputs, can lead to tacit, yet coordinated, price fixing without any direct social collusion (Bundeskartellamt & Autorité de la concurrence, 2019; Ezrachi & Stucke, 2016). This trend accelerates with emerging technologies like large language models and decentralized autonomous organizations. These technologies primarily shift the locus of control for collusive tasks from social actors to the technical subsystem—be it through agentic systems or smart contracts. The collusion taxonomy presented in this work captures the interplay between both subsystems regardless of where the locus of control is manifested, which positions the taxonomy as a useful tool for analyzing collusion patterns emerging from technological advances.

The rise of (quasi-)autonomous AI applications raises urgent new questions. As applications gain more independence in decision-making through advances in machine learning, they also gain greater capacity to facilitate or even initiate collusion (Bundeskartellamt & Autorité de la concurrence, 2019; Ezrachi & Stucke, 2016). This shift marks a new frontier: algorithmic collusion is not just a theoretical concern, it is a real and growing threat (Ezrachi & Stucke, 2016). This development necessitates a rebalancing of agency, control, and enforcement tools—a challenge that governments are already preparing for (Bundeskartellamt & Autorité de la concurrence, 2019). Technological autonomy must be accompanied by greater accountability, human oversight, and regulatory safeguards.

## 5.2. Contributions

Our main goal is to help researchers and practitioners better understand and defend against the many forms of collusion in IS. *First*, we propose a taxonomy that describes the structure of collusion in IS independent of specific cases. This taxonomy supports the identification of diverse collusion types, enables their comparison, and informs the development of detection methods and system architectures designed to mitigate collusion. It also helps investigate what different forms of collusion occur across various IS, offering insights into the contextual factors that drive or inhibit them.

*Second*, by clarifying the key dimensions and characteristics of collusion structures, the taxonomy provides practical value to system designers, security analysts, and policymakers by supporting the detection and mitigation of collusion threats beyond familiar scenarios. For example, the identified dimensions and characteristics showcase features that should be considered in the development of collusion detection approaches. Moreover, the dimensions and characteristics inform system designers of potential collusion threats.

*Third*, the collusion taxonomy lays the groundwork to contextualize collusion in IS security. Anchored in the conceptualization of collusion in IS (Section 2.1), it advances theory by framing collusion as a dysfunctional affording–constraining relationship. The taxonomy provides a structural basis for examining how collusion exploits sociotechnical affordances, circumvents constraints, and materializes through equifinal structural pathways. By linking this theoretical lens to the structural taxonomy, our work establishes a foundation not only to describe collusion in IS but also to theorize how it can emerge across different IS designs and purposes.

## 5.3. Limitations

While the literature analysis provided broad coverage, it may have missed nuanced subtopics, meaning the taxonomy may not be fully exhaustive despite reaching theoretical saturation.

The analysis is grounded in a relatively small set of legal cases from only U.S. and EU jurisdictions, which limits its generalizability to other regulatory and cultural contexts. Some identified characteristics could not be empirically confirmed and were removed, though they may still apply to real-world cases. Even reliable sources (e.g., official legal case filings) often lacked the sociotechnical detail required for comprehensive classification. Consequently, the taxonomy serves as a robust foundation, but not every real-world case can be perfectly mapped without interpretation.

## 5.4. Future Research

Collusion research is growing, but its complexity leaves much to explore, especially in IS research. By shifting focus to examining its full lifecycle—formation, execution, and dissolution—future research could provide deeper insights into why and how collusion occurs. Such research should examine not only the goals and incentives of colluders but also the IS characteristics that drive collusion. Uncovering such characteristics and mapping them to specific types of collusion will help design IS that mitigate collusion. Relevant IS characteristics might include: (1) the degree of decentralization of IS—potentially fostering horizontal collusion when high, or vertical collusion when low; (2) the anonymity of social actors; and (3) the autonomy of technical artifacts, particularly artificial intelligence. Linking collusive behavior to exploited IS characteristics could inform the selection of detection and mitigation mechanisms. Pursuing these directions presents major methodological challenges, as collecting enough detail to categorize collusion cases is difficult and time-consuming. A public, well-curated repository of collusion reports with taxonomy-based details would greatly advance research.

## Acknowledgements

We thank Sascha Rank for his valuable support. This work was supported by funding from the topic Engineering Secure Systems of the Helmholtz Association and KASTEL Security Research Labs.

## References

Bai, J., Heese, H. S., & Tripathy, M. (2023). Hiding in plain sight: Surge pricing and strategic providers. *Production and Operations Management*, *32*(12), 3837–3855.

Bajari, P., & Summers, G. (2002). Detecting collusion in procurement auctions. *Antitrust LJ*, *70*, 143.

Bundeskartellamt & Autorité de la concurrence. (2019). *Algorithms and competition* (tech. rep.). Bundeskartellamt and Autorité de la concurrence. Retrieved June 2, 2025, from https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Berichte/Algorithms_and_Competition_Working-Paper.pdf

Chatterjee, S., Sarker, S., Lee, M. J., Xiao, X., & Elbanna, A. (2021). A possible conceptualization of the information systems artifact: A general systems theory perspective. *Information Systems Journal*, *31*(4), 550–578.

Ciccarelli, G., & Lo Cigno, R. (2011). Collusion in peer-to-peer systems. *Computer Networks*, *55*(15), 3517–3532.

EC. (2001). Case at.37614 – interbrew and alken-maes [Prohibition Decision.]. Retrieved May 12, 2025, from https://competition-cases.ec.europa.eu/cases/AT.37614

EC. (2004). Case at.38359 – electrical and mechanical carbon and graphite products [Prohibition Decision.]. Retrieved May 12, 2025, from https://competition-cases.ec.europa.eu/cases/AT.38359

EC. (2014). Case at.39610 – power cables [Prohibition Decision.]. Retrieved May 12, 2025, from https://competition-cases.ec.europa.eu/cases/AT.39610

EC. (2021). Case at.39861 – yen interest rate derivatives [Prohibition Decision.]. Retrieved May 12, 2025, from https://competition-cases.ec.europa.eu/cases/AT.39861

Ezrachi, A., & Stucke, M. E. (2016). *Virtual competition* (Vol. 7). Oxford University Press.

Hagberg, A. A., Schult, D. A., & Swart, P. J. (2008). Exploring network structure, dynamics, and function using networkx. In G. Varoquaux, T. Vaught, & J. Millman (Eds.), *Proceedings of the 7th python in science conference* (pp. 11–15).

Kerr, R., & Cohen, R. (2011). Detecting and identifying coalitions. *Workshops at the Twenty-Fifth AAAI Conference on Artificial Intelligence*.

Kofman, F., & Lawarrée, J. (1993). Collusion in hierarchical agency. *Econometrica*, *61*(3), 629–656.

Laasonen, J., Knuutila, T., & Smed, J. (2011). Eliciting collusion features. *Proceedings of the 4th International ICST Conference on Simulation Tools and Techniques*, 296–303.

Laffont, J.-J., & Martimort, D. (1998). Collusion and delegation. *The RAND Journal of Economics*, *29*(2), 280–305.

Nickerson, R. C., Varshney, U., & Muntermann, J. (2013). A method for taxonomy development and its application in information systems. *European Journal of Information Systems*, *22*, 336–359.

Schwalbe, U. (2019). Algorithms, machine learning, and collusion. *Journal of Competition Law & Economics*, *14*(4), 568–607.

U.S. DoJ. (2004). U.s. v. american airlines [2004] [Competitive Impact Statement.]. Retrieved May 12, 2025, from https://www.justice.gov/atr/case/us-v-american-airlines-2004

U.S. DoJ. (2007). U.s. v. microsoft corporation (browser and middleware) [Court's Findings of Fact.]. Retrieved June 13, 2025, from https://www.justice.gov/atr/case/us-v-microsoft-corporation-browser-and-middleware

U.S. DoJ. (2023). U.s. v. activision blizzard, inc. [Competitive Impact Statement.]. Retrieved May 12, 2025, from https://www.justice.gov/atr/case/us-v-activision-blizzard-inc

U.S. DoJ. (2025). U.s. and plaintiff states v. realpage, inc. [Competitive Impact Statement.]. Retrieved May 12, 2025, from https://www.justice.gov/atr/case/us-and-plaintiff-states-v-realpage-inc

Villamil, I., Kertész, J., & Fazekas, M. (2024). Collusion risk in corporate networks. *Scientific Reports*, *14*(1), 3161.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS quarterly*, xiii–xxiii.

Wu, S., Chen, Y., Wang, Q., Li, M., Wang, C., & Luo, X. (2018). Cream: A smart contract enabled collusion-resistant e-auction. *IEEE Transactions on Information Forensics and Security*, *14*(7), 1687–1701.