TELAAH BISNIS
Volume 26, Issue 1, 11-25
http://journal.stimykpn.ac.id/index.php/tb
ISSN 1411-6375 (Print)
ISSN 2541-6790 (Electronic)

Dark Patterns Reconsidered: A Cross-Taxonomic and Conceptual Mapping for Ethical Interface Design

Onni Meirezaldi✉
Universitas Brawijaya, Indonesia

Correspondence
meirezaldi@ub.ac.id

Received May 22, 2025
Revised Jul 8, 2025
Accepted Jul 14, 2025
Published Jul 28, 2025

DOI 10.35917/tb.v26i1.586

Abstract
Dark patterns, manipulative interface strategies that steer users toward actions contrary to their interests, have become ingrained in commerce, social media, and data-collection flows. Research and regulation still lack a shared vocabulary for identifying and addressing them. This study aims to close that gap by proposing a comprehensive conceptual definition and a reconciled taxonomic map that clarifies how dark patterns operate and why they negatively impact users. Based on a directed literature review of 54 peer-reviewed sources indexed in Scopus, the analysis identifies four foundational elements: manipulative intent, information asymmetry, constrained choice, and exploitation of cognitive bias. It combines them into a single definition that unites legal, psychological, and HCI perspectives. It then cross-compares the leading taxonomies of Brignull et al., Grey et al., Mathur et al., and Zagal et al., demonstrating agreement on five mechanism families, namely Obstruction, Sneaking, Interface Interference, Forced Action, Nagging, while highlighting differing focuses on functional harms. To address this issue, the article introduces a two-dimensional grid that overlays those mechanisms with four functional areas: Finance, Privacy, Time Capture, and Psychological Pressure, creating a flexible framework capable of classifying both traditional and emerging dark-pattern strategies. The resulting model offers scholars a stable analytical framework for theory building, supplies regulators with enforceable categories for consumer protection, and equips designers with a diagnostic tool for auditing interface ethics. The study establishes a conceptual foundation for future empirical measurement, automated detection, and evidence-based policy to foster a more transparent and autonomy-respecting digital ecosystem by unifying disparate definitions and rationalizing taxonomies.
Keywords: dark patterns, deceptive design, conceptual definition, ethical design, consumer protection

Introduction

Dark patterns, manipulative interface strategies that steer users toward choices beneficial to the provider rather than the user, have become a common aspect of contemporary digital life, appearing in e commerce check outs, cookie banners, mobile games, and streaming dashboards alike (Mathur *et al.*, 2019; Radesky *et al.*, 2022). Their rapid spread is propelled by data driven business models that transform every click into monetizable insight. At the same time, advances in persuasive technology make subtle cognitive nudges technically easy and commercially tempting (Gray *et al.*, 2021). As consumers spend ever more time inside algorithmically driven environments, the line between helpful personalization and exploitative pressure blurs, heightening public concern and drawing the attention of regulators on both sides of the ocean (Leiser *et al.*, 2022; Di Porto & Egberts, 2023). Despite mounting scholarly and policy interest, achieving conceptual clarity continues to be difficult. Early commentaries

introduced the term “dark patterns” mainly through practitioner anecdotes, but later empirical work revealed definitional fault lines. Some scholars prioritize intent, framing dark patterns as “malicious interfaces that trick or force end users” (Hidaka *et al.*, 2023), whereas others highlight outcomes that “benefit the designer at the expense of the user” (Radesky *et al.*, 2022) or emphasize violations on autonomy and informed consent (Luguri & Strahilevitz, 2021). This variety of perspectives complicates cumulative knowledge building: when the same tactic can be labelled deception, coercion, or simply aggressive marketing, comparing findings across studies, or drafting legal text, becomes difficult (Kollmer & Eckhardt, 2023).

A similar fragmentation is visible in taxonomy work. Brignull’s original practitioner list popularized vivid terms such as “Roach Motel” and “Bait and Switch.” However, later research proposed function-based families (e.g., obstruction, sneaking, forced action) (Mathur *et al.*, 2019), context specific clusters (e.g., attention theft in social media, privacy erosion in consent dialogs) (Gray *et al.*, 2021), and multidimensional schemes that mix motive, mechanism, and harm (Sin *et al.*, 2025). While this diversity enhances descriptive detail, it produces overlapping or conflicting categories that hinder reliable detection and comparative impact assessment (Nazarov & Baimukhambetov, 2022; Hidaka *et al.*, 2023). As a result, policy drafters struggle to specify prohibited techniques, enforcement agencies face evidentiary challenges, and designers lack a stable reference vocabulary.

Against this backdrop, the present article pursues two interconnected objectives. First, it integrates the scattered definitional discourse to propose a comprehensive conceptual definition that captures the shared core of manipulation while acknowledging boundary conditions and variations in harm. Second, it outlines the existing taxonomic landscape, identifies points of convergence and divergence, and offers a unifying framework capable of accommodating domain specific extensions without sacrificing overall coherence. The article aims to provide an interdisciplinary benchmark for future empirical, technical, and normative work by combining insights from human-computer interaction, consumer psychology, media studies, and legal scholarship.

The theoretical significance of this effort is threefold. It provides a reliable conceptual scaffold that supports cumulative research across methods and disciplines; it clarifies the relationship between dark patterns and related constructs such as deceptive design, nudging, and persuasive technology, thus preventing terminological confusion; and it supplies measurement scholars with clear inclusion criteria, which is essential for cultivating robust prevalence metrics and causal models (Luguri & Strahilevitz, 2021; Mathur *et al.*, 2021). Practically, a shared definition and standardized taxonomy can assist interface auditors and AI based detectors in identifying harmful design practices with greater precision (Kirkman *et al.*, 2023); inform regulatory drafting by translating abstract consumer protection principles into actionable categories (Leiser *et al.*, 2022); and guide product teams toward transparency oriented alternatives, thereby helping firms balance commercial goals with user trust and sustained loyalty (Lu *et al.*, 2024).

Dark patterns have evolved from niche UX curiosities into a systemic challenge that involves ethics, economics, and public policy. Yet the field’s conceptual foundations lag behind its practical demands. By consolidating definitions and rationalizing taxonomies, this study aims to equip scholars, practitioners, and regulators with a common language for diagnosing, debating, and ultimately controlling manipulative design. The following sections elaborate on the methodological approach and present the resulting integrative framework, paving the way for more coherent scholarship and effective protection in the digital marketplace.

Literature Review

Dark patterns, often defined as deceptive or manipulative design practices embedded within digital interfaces, have become an increasingly central subject in human-computer interaction, behavioral economics, and consumer protection studies. The foundational concept was introduced by Brignull in 2010, who described dark patterns as design strategies that mislead or coerce users into actions that they would not otherwise choose (Brignull *et al.*, 2023). Since then, scholarship has expanded the definitional and taxonomic understanding of dark patterns, exploring their mechanisms, psychological foundations, and ethical implications.

Across the literature, a consistent definition emerges: dark patterns are intentionally crafted interface configurations that exploit predictable cognitive biases and information asymmetries to push users toward outcomes that serve the service provider's interest, often at the expense of user autonomy or welfare (Mathur *et al.*, 2019; Gray *et al.*, 2021; Hidaka *et al.*, 2023). These designs rely on four core fundamental elements: manipulative intent, information asymmetry, constrained choice, and cognitive bias exploitation. Each element has been differently emphasized in academic definitions, but their combination underlies the manipulative power of dark patterns.

The terminology associated with dark patterns also reflects the field's evolution. While "dark patterns" remains the most widely recognized term, alternative expressions such as "deceptive design," "manipulative UX," and "coercive interfaces" emphasize different aspects, legal deception, psychological manipulation, and autonomy infringement respectively (Leiser *et al.*, 2022; Di Porto & Egberts, 2023). These overlapping yet distinct terminologies highlight the interdisciplinary nature of the phenomenon and the challenges of regulatory and empirical unification.

The taxonomic mapping of dark patterns further enriches this discussion. Brignull's original typology, though illustrative, lacked analytic depth. Subsequent refinements by Zagal *et al.* (2013), Mathur *et al.* (2019), and Gray *et al.* (2021) introduced structured families such as Obstruction, Sneaking, Interface Interference, Forced Action, and Nagging, each tied to distinct manipulation methods. This structural classification has proven essential for both empirical auditing (e.g., web crawls) and regulatory interventions. Furthermore, recent studies emphasize functional taxonomies that link dark patterns to harm domains, namely Finance, Privacy, Time Capture, and Psychological Pressure, providing a multidimensional view of their societal impact.

Behavioral and user design theories offer a comprehensive understanding on the effectiveness of dark patterns. Cognitive Load Theory (Zhang & Gao, 2022), and Persuasive Design (Naslund *et al.*, 2017) explain how interface choices exploits users' bounded rationality and cognitive limitations. For example, dark patterns exploit default effects, decision fatigue, and emotional triggers like urgency or scarcity (Krisam *et al.*, 2021; Esposito & Ferreira, 2024), thereby overriding users' reflective thought processes. The Elaboration Likelihood Model (Kompaniets & Chemerys, 2019) and Dual Process Theory (Baxter *et al.*, 2025) also support the idea that dark patterns steer users through peripheral rather than central processing routes, increasing susceptibility to manipulation.

These manipulations have significantly impact user satisfaction, loyalty, and perceptions of corporate ethics. Studies by Luguri & Strahilevitz (2021), Akbar & Nurmahdi (2019), and Hilton (2023) demonstrate that dark patterns diminish trust, reduce user satisfaction, and negatively affect long-term engagement. Theoretical frameworks like Expectation Confirmation Theory and the Technology Acceptance Model help explain these dynamics by showing how unmet user expectations or decreased perceived usefulness lead to dissatisfaction and reduced loyalty (White, 2015; Khair, 2025). Furthermore, empirical studies link dark patterns to broader ethical assessments, indicating that users view companies

employing such tactics as less trustworthy and more focused on profit (Brunk, 2010; Singh *et al.*, 2024).

At the organizational level, the motivations for deploying dark patterns are complex. Companies pursue revenue optimization, user retention, operational efficiency, and enhanced data collection through these strategies (Mathur *et al.*, 2019; Kitkowska *et al.*, 2022). Patterns like forced continuity, hidden charges, and pre-selected options are frequently utilized in subscription-based services to ensure monetization through friction-laden opt-out processes (Bajaj et al., 2025; Jain et al., 2025). While effective in the short term, these practices may lead to reputational and regulatory backlash in the long term, sparking demands for enforceable design standards.

Methodologically, research on dark patterns has adopted a variety of approaches. Exploratory methods (Kitkowska *et al.*, 2022), quantitative surveys (Mathur *et al.*, 2019; Sin *et al.*, 2025), case studies (Machuletz & Böhme, 2020), and experiments (Voigt *et al.*, 2021) provide valuable insights into user experiences and behavioral responses. Content analysis and automated scraping tools have expanded the empirical reach of the field (Krisam *et al.*, 2021; Mathur *et al.*, 2021), while instruments like the System Darkness Scale (van Nimwegen *et al.*, 2022) and Dark Patterns Identification Scale (Bessant *et al.*, 2023) offer standardized means for measuring exposure and evaluating design ethics.

Despite these advances, a conceptual and taxonomic fragmentation persists, complicating enforcement, empirical comparison, and ethical accountability. The present study addresses this gap by synthesizing a cohesive definition and proposing a two-dimensional framework that categorizes dark patterns by both mechanism and functional harm. This integrative approach aims to support theory development, regulatory drafting, and ethical interface auditing in an increasingly immersive digital environment.

Research Method

This study utilizes a directed literature-review strategy based on a conceptual analysis orientation. A directed review starts from an a predetermined set of sensitizing constructs, in this case, the definitional ambiguities, competing taxonomies, and ethical debates documented in the dark-patterns corpus, and progressively refines them as new evidence is encountered (Mathur *et al.*, 2019; Gray *et al.*, 2021). Unlike a systematic review that thoroughly maps an entire field, a directed review emphasizes theoretical depth over breadth, seeking to resolve conceptual conflicts rather than enumerate every paper. The review, however, was executed with procedural rigor to maximize transparency and reproducibility: search queries, screening decisions and coding templates were recorded in a shared protocol that can be audited alongside this article.

All bibliographic retrievals were conducted in March 2025, selected for its multidisciplinary coverage of computer science, psychology, media studies and marketing strategies. Searches combined controlled vocabulary and free-text strings derived from the previous keyword inventory provided for the present project. The final search expression concatenated five Boolean blocks joined with AND: (1) concept identifiers, “dark patterns” OR “deceptive design” OR “manipulative interface” OR “coercive UX”; (2) conceptual focus, “definition” OR “taxonomy” OR “classification” OR “typology” OR “conceptual framework”; (3) adjacent constructs, “persuasive design” OR “nudging” OR “choice architecture”; (4) ethical or regulatory qualifiers, “ethics” OR “autonomy” OR “privacy” OR “regulation” OR “GDPR”; and (5) impact terms, “user perception” OR “trust” OR “consumer welfare”. To capture grey literature impacting scholarly discourse, we added the derivative string (“dark patterns” AND “policy brief” OR “white paper”), but limited inclusion to documents with an ISBN, DOI or peer-review flag to ensure academic quality.

The inclusion criteria required that a record (a) offered an explicit definition or conceptual discussion of dark patterns, (b) presented or critiqued a taxonomy, or (c) analyzed ethical or regulatory implications. Empirical studies were eligible only when they used a definitional or taxonomic construct as an analytical framework, ensuring relevance to the conceptual perspective. Exclusion criteria eliminated short practitioner blog posts included in conference adjuncts, duplicate pre-print/main-version pairs, papers that mentioned dark patterns only briefly, and articles focused exclusively on dark-pattern detection algorithms without reflecting on the underlying concept (Nazarov & Baimukhambetov, 2022). After deduplication and title/abstract screening, 112 sources advanced to full-text evaluation; 54 met all criteria and comprised the analytic corpus.

Analytic coding proceeded in two cycles. First, open coding extracted verbatim definitional phrases, taxonomy labels and stated ethical concerns from each article, producing a codebook of 67 unique concepts. Second, axial coding grouped these concepts into three meta-dimensions that structure the remainder of this article. The definitional dimension captures semantic fundamentals such as intentionality, benefit asymmetry and infringement on informed consent (Luguri & Strahilevitz, 2021; Hidaka *et al.*, 2023). The typological dimension groups the multitude of labels into functional families, obstruction, sneaking, interface interference and forced action, while noting unresolved overlaps and new categories tied to immersive media or AI-driven personalization (Mathur *et al.*, 2019; Krauß *et al.*, 2024). The ethical-implication dimension integrates normative evaluations, spanning autonomy erosion, collective welfare loss and regulatory legitimacy (Leiser *et al.*, 2022; Di Porto & Egberts, 2023).

Throughout coding, a constant-comparison approach was applied: any new statement was compared against existing categories to determine if it needed a new code or improved an existing one. Memo writing captured theoretical insights and identified tensions, such as whether intent or outcome should dominate the definition, influencing the ongoing adjustment of inclusion criteria and search queries. Reliability was enhanced through independent duplication of 20 per cent of coding decisions, achieving Cohen's $\kappa = 0.82$; discussion resolved discrepancies.

Synthesizing across the three dimensions creates a coherent scaffold that clarifies how scholars describe dark patterns, how they appear, and why they matter ethically. This framework serves as the analytical lens for the following findings: first, a reconciled definition derived from convergent elements across sources; second, an integrative taxonomy that nests existing schemes within a unifying hierarchy; and third, an ethical appraisal that situates dark patterns at the intersection of designer intent, user vulnerability and regulatory accountability.

Discussion

The Evolution of Definitions and Terminology

The term "dark patterns" entered the lexicon of digital design criticism in 2010, when UX practitioner Harry Brignull launched the website darkpatterns.org to expose interface tactics that "mislead or coerce users into doing things they wouldn't otherwise do" (Brignull *et al.*, 2023). Brignull's blog style taxonomy, featuring memorable labels such as "Bait and Switch" and "Roach Motel", quickly travelled from design meetups into academic settings, providing researchers with a vivid umbrella term for manipulative choice architectures that had long existed but lacked a shared name. Its impact stemmed from the moral clarity of the adjective "dark," which framed deception not as a functional flaw but as a deliberate ethical violation. Yet, the term's activist origins also meant that its conceptual framework being outlined more by illustrative anecdotes than by systematic theorizing.

As academic interest accelerated, parallel labels emerged that attempted to either narrow or broaden the original concept. Deceptive design emphasizes the intention to mislead and is widely used in legal and policy writing because it aligns with consumer protection statutes that prohibit deception (Di Porto & Egberts, 2023). Manipulative UX redirects focus from designer intent to psychological impact, emphasizing how interface elements exploit cognitive biases to influence behavior (Gray *et al.*, 2021). Coercive interface borrows language from political philosophy, suggesting an erosion of user autonomy severe enough to resemble coercion rather than mere persuasion (Leiser *et al.*, 2022). Each term encompasses a different normative angle, legal deception, psychological manipulation, autonomy infringement, and each consequently sets a slightly different evidentiary bar for identifying misconduct. The abundance of synonyms reflects the field's interdisciplinary nature, but it also creates confusion when studies use different labels for overlapping phenomena, complicating meta-analyses and regulatory drafting.

Examining key academic definitions illustrates how these terminological nuances play out. Brignull's original description, while forceful, relied on everyday verbs such as "trick" and "mislead," providing moral color yet little operational clarity. Mathur *et al.* (2019) refined the language by defining dark patterns as "user interface designs that benefit an online service by coercing, steering, or deceiving users into making unintended decisions," thereby identifying three mechanism verbs, namely coercion, steering, and deception, and explicitly connecting them to organizational benefit. This formulation enhanced analytical value in two respects: first, it framed dark patterns as design choices rather than isolated elements, and second, it embedded outcome (unintended user decisions) alongside intent (benefit to the service). However, including "steering" raised boundary issues: could soft defaults that merely nudge, without hiding information, qualify as dark if they also lead to beneficial outcomes for users?

Gray *et al.* (2021) responded by emphasizing felt experience, labelling dark patterns "interface practices perceived by users as manipulative, deceptive, or coercive." The strength of this perspective lies in its phenomenological awareness; it can capture patterns whose manipulativeness becomes evident only through user testimony. Yet its reliance on perception present methodological challenges: users vary in expertise and tolerance, meaning a practice might be deemed dark by one group and neutral by another, complicating enforcement and detection algorithms aiming for universal criteria. In addition, Grey et al. examined the ethical dimension of interface design from a human-computer interaction perspective, suggesting that dark patterns may systematically exploit known cognitive vulnerabilities to promote conflicting interests. This framing contributes theoretical depth by aligning with behavioral economics, although it introduces evidentiary challenges in demonstrating designer intent. The dilemma from the standpoint of human computer interaction ethics suggest that dark patterns are interface design strategies that exploit well-documented cognitive biases to benefit providers at the user's expense, a view supported by Gray *et al.* (2021) in their analysis of manipulative user experiences. This wording supports the concept of systematicity, isolating accidental design mishaps from strategic manipulation, and explicitly links malalignment with cognitive science. Its advantage is theoretical depth, aligning with behavioral economics insights about bounded rationality; its drawback is evidential: proving that designers had knowledge of a cognitive vulnerability and applied it systematically can be challenging in practice.

Hidaka *et al.* (2023) tightened the focus on malicious intent, referring to dark patterns "malicious interface design patterns that trick or force end users into actions benefiting the purveyor." The definition aligns with cybersecurity language by highlighting malice, emphasizing responsibility and facilitating legal sanction. Yet critics argue that malice is difficult to infer; many conversion optimization methods evolve gradually without a clear

intent to cause harm, and excessive emphasis on malice could let harmful but "well meaning" designs escape scrutiny.

A cross-definition synthesis reveals shared elements worth retaining. Almost all descriptions reference (1) a designer or organizational beneficiary, (2) an asymmetry of benefit or power, (3) a user action not freely chosen, and (4) a mechanism of deception, coercion, or exploitation of cognitive bias. Differences arise over the weight assigned to intent versus outcome and over the threshold at which persuasive design crosses into manipulation. Definitions prioritizing intent provides clearer moral accountability but may overlook certain cases; outcome-oriented definitions capture a broader universe of harmful effects but can also include innocent nudges. Perception based definitions center user experience but suffer from subjectivity, while cognitive vulnerability framings add scientific rigor yet complicate evidentiary standards.

Evaluating these strengths and weaknesses suggests three criteria for a strong conceptualization. First, normative clarity: the definition should explain why the pattern is wrong, be it deception, autonomy violation, or welfare loss, while avoiding purely emotive language. Second, operational tractability: researchers and regulators must be able to implement the definition using observable interface properties or user outcomes. Third, contextual adaptability: as interfaces transition into virtual reality headsets and AI driven voice agents, the definition must scale to formats where visual cues are absent and manipulation operates through timing, tone, or data asymmetry (Krauß *et al.*, 2024).

Considering this critical evaluation, many scholars now support hybrid formulations that intersect intent, mechanism, and effect. Mathur *et al.* (2021) move in this direction by asking, "What makes a dark pattern… dark?" and proposing evaluative criteria, such as foreseeability of harm, inability to avoid reasonably, and disproportionate benefit to the provider. These criteria reflect the deceptive practices test in U.S. consumer law, bridging academic taxonomy with enforceable standards. Yet the question of user consent is still debated: can an interface still harbor dark patterns if exhaustive information is available but cognitively overwhelming? Here, the coercive interface camp argues that informational overload amounts to manipulation, because rational evaluation becomes infeasible (Leiser *et al.*, 2022).

The definitional debate thus reflects underlying conflicts between libertarian and paternalistic philosophies of design governance. Brignull's activist term highlighted moral outrage; later academic refinements seek analytical precision while maintaining normative force. Progress depends on integrating the diverse focuses, such as intentional deception, cognitive exploitation, experiential harm, into a structured model that accommodates varying evidentiary contexts while retaining a common moral core. Such a model would not eliminate grey areas. However, it would provide scholars, auditors, and legislators with a clearer guide for navigating a design environment where the next manipulative tactic is only a split test away.

Core Conceptual Elements of Dark Patterns

The conceptual framework of a dark pattern rests on a small set of recurring building blocks that appear, in varying combinations, across nearly all scholarly definition. First is manipulative intent: the design is crafted to advance the provider's interests, not just to facilitate use. Brignull's original manifesto called for "tricking" the user. At the same time, later legal framings speak of "deception" or "coercion," yet all converge on the idea that the designer's purpose is to secure outcomes the user is unlikely to choose independently. Second is information asymmetry: critical details, including price increments, data sharing consequences, cancellation pathways, are obscured, delayed, or fragmented so that users cannot accurately weigh costs and benefits. Third comes constrained choice architecture: although alternatives technically exist, the interface selects them cognitively or procedurally burdensome, tilting

behavior toward the designer's preferred option. Finally, exploitation of cognitive biases supplies the psychological engine: scarcity cues enhance loss aversion, pre ticked boxes harness default effects, and visually dominant CTAs capture attentional bias. Together, these elements transform what could have been a neutral nudge into a form of digital manipulation. The extent to which each element is emphasized differs by author and discipline. This variation is summarized in Table 1, which correlates representative definitions against the four core elements. Brignull's definition stresses intent and constrained choice but does not explicitly mention cognitive science. Mathur *et al.* (2019) explicitly link manipulation to organizational benefit and detail asymmetry and bias exploitation, providing an early behavioral economics turn. Gray *et al.* (2021) add the experiential dimension, anchoring the pattern's darkness in how users feel its manipulative pull, while Hidaka et al. introduce the familiar language of malice found in cybersecurity. Greenberg and Buxton, writing from an HCI perspective, foreground systemic exploitation of known cognitive vulnerabilities, highlighting the bias and insisting on repeated, rather than accidental, deployment. Finally, Luguri & Strahilevitz (2021) emphasize the legal doctrine of "material distortion" of choice, which is triggered when asymmetry and constrained design jointly deprive the user of meaningful consent.

Table 1 shows that every author acknowledges manipulative intent but differs in which supporting mechanisms they prioritize. Legal scholarship (Luguri & Strahilevitz, 2021) emphasizes information asymmetry as the decisive trigger for "material distortion," whereas HCI perspectives (Hidaka *et al.*, 2023) classify malicious intent itself as the core diagnostic. Gray *et al.* (2021) incorporate cognitive bias mainly through users' felt manipulation, while Brignull's original practitioner perspective entirely excludes the psychological dimension.

Table 1. Core conceptual elements emphasized in leading dark pattern definitions

Definition / Source	Manipulative Intent	Information Asymmetry	Constrained Choice	Cognitive-Bias Exploitation
Brignull *et al.* (2023)	✓	–	✓	–
Mathur *et al.* (2019)	✓	✓	✓	✓
Gray *et al.* (2021)	✓	✓	✓	△
Hidaka *et al.* (2023)	●	✓	✓	✓
Luguri & Strahilevitz (2021)	✓	●	✓	✓

Legend
● — singled out as the keystone of the definition
✓ — explicitly articulated element
△ — acknowledged indirectly (e.g., through user-experience evidence)
– — not foregrounded / only implicit

Based on the similarities in Table 1, this article proposes the following comprehensive definition: A dark pattern is a deliberately engineered configuration of interface elements that leverages information asymmetry and exploits predictable cognitive biases to channel users toward choices that disproportionately benefit the designer, while burdening alternative actions with hidden or excessive friction, thereby undermining informed and autonomous decision making. This formulation captures manipulative purpose ("deliberately engineered"), operational mechanism (asymmetry and bias), structural implementation (friction laden alternatives), and normative consequence (erosion of autonomy). It also scales across modalities: regardless of whether the channel is visual, auditory, or haptic, the presence of engineered asymmetry combined with exploitative friction remains detectable.

By combining the strongest aspects of previous definitions, Brignull's moral clarity, Mathur's benefit criterion, Gray's user perspective, and Luguri & Strahilevitz's material distortion threshold, the integrated definition aims to provide researchers with a stable analytical foundation, regulators with enforceable language, and designers with a clear ethical

boundary. Future sections put this definition through a reconciled taxonomy and examine how each element manifests across interface genres from cookie banners to extended reality menus.

Mapping the Taxonomic Landscape of Dark Patterns

Since Brignull's first catalogue, researchers have moved from impactful anecdotal labels to structured typologies that expose manipulative design's mechanics, contexts, and harms. The four most influential schemes, Brignull *et al.* (2023), Gray *et al.* (2021), Mathur *et al.* (2019), and Zagal *et al.* (2013), exhibit familial resemblances yet vary in detail and domain focus, producing a complex picture that can confuse newcomers and regulators alike.

Brignull's list functions as the root node: thirteen named tricks, including Bait and Switch and Roach Motel, illustrate how interface friction or misdirection undermines user intent. The taxonomy owes its popularity to memorable metaphors and direct connections to everyday shopping pain points, but it is still more flat and illustrative than analytic; categories overlap and lack explicit criteria.

Gray *et al.* (2021) restructured Brignull's anecdotes into five super families, namely Obstruction, Sneaking, Interface Interference, Forced Action, and Nagging, derived from a qualitative synthesis of 73 peer reviewed articles. Obstruction involves routes that deliberately hinder normal actions (e.g., labyrinthine unsubscribe flows). Sneaking hides relevant information, including fees, permissions, or default opt ins, until the commitment feels irreversible. Interface interference manipulates visual hierarchy, wording, or timing so that the designer's preferred path appears prominent or urgent. At the same time, Forced Action restricts access or functionality unless the user complies with unrelated requests. The fifth category, Nagging, captures persistent prompts that wear down resistance. Gray's strength is parsimony and transferability: each family is defined by the mechanism rather than platform specifics, facilitating the identification emerging patterns in new media.

Mathur *et al.* (2019) introduce a multidimensional lens by cross-referencing mechanisms (steering, coercion, deception) with harm loci such as privacy, finance, or attention. Their extensive crawl of 11k shopping sites revealed 1,818 instances of dark patterns demonstrating that seemingly distinct tricks cluster around shared goals. This data driven refinement offers empirical significance, but its broad mechanism labels sometimes weaken interpretive precision, steering and coercion can merge when both interface friction and emotional pressure occur together.

Zagal *et al.* (2013) brough the debate into digital games, emphasizing temporal and monetary exploitation. Their typology distinguishes soft monetization (cosmetic micro transactions) from hard paywalls and differentiates voluntary time investments (collectathons) from forced grinds designed to sell boosts. Although focused on games, the framework highlights a neglected aspect, time capture, that also underlies binge watch loops on streaming platforms and endless scroll social feeds.

Table 2. Convergence of Major Taxonomies on Core Dark Pattern Families

Taxonomy	Obstruction	Sneaking	Interface Interference	Forced Action	Nagging/ Persuasive Nudge	Financial Exploit	Temporal Exploit
Brignull (2010)	✓ (Roach Motel)	✓ (Hidden Costs)	✓ (Misdirection)	✓ (Forced Continuity)	–	✓	Δ
Gray et al. (2021)	✓	✓	✓	✓	✓	Δ	Δ
Mathur et al. (2019)	✓	✓	✓	✓	–	✓	Δ
Zagal et al. (2013)	Δ	✓	Δ	✓	–	✓	✓

✓present and explicitly named Δ present but implicit/secondary.

The matrix demonstrates that all schemes acknowledge obstruction, sneaking, interface interference and forced action; divergence lies in whether "persistent persuasion" (nagging) or time capture earn independent status. Financial exploitation appears throughout, whereas temporal exploitation only stands out in game and media contexts. This visual juxtaposition highlights where definitions overlap, where they specialize, and where analytical gaps persist, particularly concerning emerging attention harvesting loops.

A proposed function-oriented extension

To merge overlap and integrate newer digital contexts, we propose layering the existing mechanism families onto four functional domains:

- Financial manipulation – patterns that generate direct monetary outflow or hinder cost comparison (e.g., drip pricing during checkout, involuntary auto renewal).
- Privacy erosion – patterns that extract or monetize data (e.g., pre ticked consent boxes, convoluted opt out paths).
- Time capture – patterns that maximize session length or return visits by exploiting temporal scarcity, infinite scroll, or autoplay.
- Psychological pressure – patterns that weaponize affect, guilt, or social proof (e.g., confirm shaming, fake countdowns, inflated popularity cues).

Each instance of a dark pattern can thus be coded on two axes: mechanism (Obstruction, Sneaking, Interface Interference, Forced Action, Nagging) and function (Finance, Privacy, Time, Psychology). A roach motel unsubscribe flow becomes [Obstruction × Finance]; autoplay with no easy off ramp is [Forced Action × Time]; a guilt laden "No, I like full price!" prompt is [Nagging × Psychology]. This bivariate grid simplifies comparative research, highlights context specific risks, e.g., time capture harms in children's apps compared to privacy erosion in ad tech, and assists regulators in aligning obligations to harm domains rather than chasing an expanding list of identified tricks.

Theoretical and Practical Implications

Research on dark patterns reshapes several disciplinary conversations at once, including human computer interaction (HCI), design ethics, behavioral economics, consumer protection law, and public policy studies, by demonstrating how seemingly "usable" interfaces can be manipulated to undermine autonomy and redistribute welfare from users to service providers. Theoretically, the concept forces HCI to enhance its classic triad of efficiency, effectiveness, and satisfaction by adding a fourth dimension: integrity of intent. Brignull's early investigations and the phenomenological testimonies collected by Gray *et al.* (2021) reveal that an interaction can satisfy ISO usability heuristics while still violating core ethical principles if engineered to deceive or mislead. Consequently, user-centred and value-sensitive design must develop to include explicit checks for power asymmetries, intent, and downstream societal impact.

Behavioral science scholarship likewise obtains a sharper lens on negative nudging. Where "choice architecture" research traditionally highlights how gentle defaults can encourage desirable behavior, Mathur *et al.* (2019) and subsequent extensive crawls show the same cognitive shortcuts, such as status quo bias, scarcity effects, and hyperbolic discounting, being exploited for profit extraction, data harvesting, or capturing attention. Dark pattern analysis extends bounded rationality theory by illustrating that design changes do not always enhance welfare; they can equally produce sludge that sabotages rational choice. Understanding this dual use nature of persuasive design is crucial for refining consumer decision-making models in digital contexts.

From a legal and regulatory standpoint, dark patterns reveal an enforcement blind spot. Most consumer protection statutes prohibit deception in content (false claims, omissions) but remain neutral about form, including interface elements' layout, timing, or sequencing.

Empirical studies demonstrating non-compliant cookie banners under GDPR (Nouwens *et al.*, 2020) and "obstruction" processes in e commerce unsubscribe paths (Mathur *et al.*, 2021) have prompted EU lawmakers to discuss explicit bans on manipulative choice designs in the Digital Services Act. Leiser *et al.* (2022) argues for regulatory pluralism that fuses data protection law with consumer law, because dark patterns consistently blur the line between privacy harms and commercial harms. In the United States, recent FTC policy statements similarly indicate that design practices causing "dark pattern driven" consumer injury may be prosecuted as unfair or deceptive, reflecting a transition from content centric to architecture aware jurisprudence.

These regulatory debates raise practical design issues. If free, specific, informed, and unambiguous consent is becoming the new gold standard, interface teams must implement transparency beyond static privacy policies. The functional mechanism grid proposed in this article provides product teams with a heuristic checklist: any design that pairs Sneaking × Privacy or Forced Action × Finance warrants intensive ethical review. Incorporating this taxonomy into agile design toolkits, journey maps, Figma component libraries, and design-system lint rules can provide "red-flag" cues before features reach production. Early adopter organizations (e.g., Mozilla Foundation, Centre for Humane Technology) have begun to formalize consent integrity patterns and "trust marks" that certify autonomy respecting flows, pointing toward a future where dark pattern audits are as common as accessibility scans.

The scholarship further encourages methodological innovation in detection technology. Automated scrapers and machine learning models (Kirkman *et al.*, 2023) now classify dark patterns across thousands of websites. Researchers observe that many patterns depend on cross step friction or psychological pressure not visible in static HTML. Integrating conceptual taxonomies with dynamic behavioral telemetry, click delays, back button churn, and rage clicks could raise detection accuracy and provide regulators with actionable evidence. Equally, transparency regulations could require platforms to expose interaction logs annotated with dark pattern risk scores, allowing for third party auditing and reproducible oversight.

For design education curricula, dark patterns serve as a vivid case study in professional ethics. Including scenarios of manipulative check out flows or guilt laden opt outs in UX studio courses sensitizes future professionals to the long term reputational and legal costs of short term conversion gains. Lachheb *et al.* (2023) emphasize the need for learning design programs to educate students in inclusive and privacy preserving practices and anti-manipulative design literacy. The evidence that user trust and brand loyalty deteriorate when manipulation is detected (Kollmer & Eckhardt, 2023; Singh *et al.*, 2025) reinforces the business case: ethical design is not a philanthropic add on but a strategy for risk reduction and customer lifetime value safeguard.

Finally, dark pattern research paves the way for interdisciplinary collaboration. Psychologists provide models of susceptibility; data scientists develop engineer detectors; legal scholars craft enforcement triggers; and designers translate principles into interface features. The synthetic mechanism by function grid presented here provides a common language for those collaborations, clarifying that the same exploitative objective (e.g., time capture in streaming) can be delivered through multiple tactics (autoplay, infinite scroll, nagging alerts) and, conversely, that a single interface maneuver (visual misdirection) can support several harms depending on context. Such clarity is indispensable for a balanced policy that discourages manipulation without stifling legitimate persuasion or innovation.

In conclusion, the advanced study of dark patterns reorients theory, policy, and practice toward a conception of digital design as a technical craft and a site of competing power

relations. Recognizing, classifying, and neutralizing manipulative designs will be pivotal to sustaining user trust, regulatory compliance, and ethical integrity in the next wave of pervasive computing.

Limitations and Future Research Directions

This article is intentionally conceptual and therefore carries several methodological constraints that must modulate the generalizations drawn. Most importantly, it does not report original empirical data; the synthesis relies on extant literature gathered exclusively from Scopus, which, while comprehensive, may privilege English language and Western centric scholarship, potentially overlooking design traditions and regulatory debates emerging in Latin America, Sub Saharan Africa, or East Asia. As the review focused on peer reviewed sources that emphasize definitional and taxonomic issues, practitioner blogs, industry white papers, and grey literature audits, often the earliest to document new dark pattern tactics, were excluded. That decision improves academic reliability, but may underrepresent the rapid interface experiments implemented by major platforms. Furthermore, the coding scheme treats each paper as an independent evidence unit, yet publication bias may exaggerate the visibility of spectacular or extreme patterns while understating mundane but widespread forms of manipulation. Finally, the functional overlay proposed here is derived deductively and requires validation in specific domains such as health apps, educational platforms, and voice assistant environments where interaction methods differ significantly from point and click web interfaces.

These limitations suggest a clear plan for future inquiry. First, extensive empirical mapping is needed to measure how mechanism-function combinations manifest across digital sectors, ideally combining automated interface scraping with manual coding for validation. Second, experimental and observational studies should test how specific dark patterns affect user behavior, trust, and well-being, with particular attention to psychological factors like loss aversion or default bias. Cross-cultural research can further assess variation in perceived coercion, while advancements in machine learning tools may lead toward risk scoring systems that guide regulatory triage. Finally, longitudinal studies connecting exposure to dark patterns with downstream effects, trust erosion, disengagement, or reduced lifetime value, are essential for substantiating ethical and economic concerns.

Conclusion

Dark patterns can now be succinctly defined as deliberately engineered configurations of interface elements that exploit information asymmetries and predictable cognitive biases to channel users toward choices that disproportionately benefit the provider, while burdening alternative actions with hidden or excessive friction, thereby undermining informed and autonomous decision making. This synthesis integrates the moral clarity of Brignull's original exposition, the outcome-oriented precision of Mathur *et al.* (2019), and the phenomenological sensitivity of Gray *et al.* (2021).

The taxonomic framework that surrounds this definition is clarified in two intersecting dimensions. Five families recur across the literature on the mechanism axis, namely Obstruction, Sneaking, Interface Interference, Forced Action, and Nagging, each describing how manipulation is delivered. Overlaid on this is a functional axis that clarifies why the tactic is deployed: to extract financial value, erode privacy, capture time/attention, or exert psychological pressure. Mapping real world designs onto this bivariate grid highlights reoccurring patterns, Forced Action × Privacy in consent banners, Sneaking × Finance in drip pricing check outs, Obstruction × Time in endless scroll feeds, while revealing under studied combinations that deserve empirical scrutiny.

The definition and grid provide scholars, auditors, and regulators with a shared analytic vocabulary. Yet conceptual clarity alone will not prevent manipulative design. The findings highlight an urgent need for industry wide norms that treat respect for user autonomy as a non-negotiable design constraint, similar to accessibility. Product teams should integrate dark pattern checklists into design systems and commit to provide easy opt outs, transparent defaults, and proportional data requests. Regulators can convert the mechanism by function grid into enforceable standards, ensuring that interface design, not just content, is included under consumer protection law. Educators must also embed anti manipulative design literacy into UX curricula enabling the next generation of practitioners can associate conversion metrics with ethical responsibility.

This article unifies various definitions and rationalizes taxonomies, providing a foundation for a more transparent, trustworthy, and user respecting digital environment. The current challenge is collective: to convert conceptual insight into formalized practice and policy before the next wave of immersive technology multiplies both the power and the peril of dark patterns.

References

Akbar, N. F., & Nurmahdi, D. A. (2019). Analysis of Perceived Usefulness, Perceived Ease of Use and Service Quality on User Satisfaction in Using Snaapp Communication Application in Ignatius Slamet Riyadi Karawang Elementary School. *Saudi Journal of Business and Management Studies*, *4*(11), 849-855. https://doi.org/10.36348/sjbms.2019.v04i11.005

Baxter, K. A., Sachdeva, N., & Baker, S. (2025). The Application of Cognitive Load Theory to the Design of Health and Behavior Change Programs: Principles and Recommendations. *Health Education & Behavior*, 10901981251327185. https://doi.org/10.1177/10901981251327185

Bessant, C., Ong, L. L., Cook, L. A., Hoy, M. G., Pereira, B., Fox, A., Nottingham, E., Steinberg, S., & Gan, P. (2023, Oct 18-21). Exploring Parents' Knowledge of Dark Design and Its Impact on Children's Digital Well-Being. AoIR2023: The 24th Annual Conference of the Association of Internet Researchers, Philadelphia, PA, USA. https://doi.org/10.5210/spir.v2023i0.13395

Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023). *Deceptive patterns – user interfaces designed to trick you*. Retrieved April 25 from https://www.deceptive.design/

Brunk, K. H. (2010). Exploring origins of ethical company/brand perceptions — A consumer perspective of corporate ethics. *Journal of Business Research*, *63*(3), 255-262. https://doi.org/https://doi.org/10.1016/j.jbusres.2009.03.011

Di Porto, F., & Egberts, A. (2023). The collective welfare dimension of dark patterns regulation. *Eur Law J*, *29*(1-2), 114-141. https://doi.org/10.1111/eulj.12478

Esposito, F., & Ferreira, T. M. C. (2024). Addictive Design as an Unfair Commercial Practice: The Case of Hyper-Engaging Dark Patterns. *European Journal of Risk Regulation*, *15*(4), 999-1016. https://doi.org/10.1017/err.2024.8

Gray, C. M., Santos, C., Bielova, N., Toth, M., & Clifford, D. (2021). Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, Yokohama, Japan*. https://doi.org/10.1145/3411764.3445779

Hidaka, S., Kobuki, S., Watanabe, M., & Seaborn, K. (2023). Linguistic Dead-Ends and Alphabet Soup: Finding Dark Patterns in Japanese Apps. *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, Hamburg, Germany.* https://doi.org/10.1145/3544548.3580942

Hilton, M. (2023). Dark Patterns and User Mental Health: Identifying Theoretical Impacts of Deceptive Design on Vulnerable Demographics. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *67*(1), 2124-2127. https://doi.org/10.1177/21695067231199684

Khair, M. S. (2025). Analyzing Factors Influencing Subscription Decisions for Exclusive Content on Instagram. *International Student Conference on Business, Education, Economics, Accounting, and Management (ISC-BEAM)*, *3*(1), 234-248. https://doi.org/10.21009/ISC-BEAM.013.15

Kirkman, D., Vaniea, K., & Woods, D. W. (2023, 3-7 July 2023). DarkDialogs: Automated detection of 10 dark patterns on cookie dialogs. 2023 *IEEE 8th European Symposium on Security and Privacy (EuroS&P), Delft, Netherlands.* https://doi.org/10.1109/EuroSP57164.2023.00055

Kitkowska, A., Högberg, J., & Wästlund, E. (2022, January, 3-7). Barriers to a well-functioning digital market: Exploring dark patterns and how to overcome them. *55th Hawaii International Conference on System Sciences, Manoa, University of Hawai'i.*

Kollmer, T., & Eckhardt, A. (2023). Dark Patterns. *Business & Information Systems Engineering*, *65*(2), 201-208. https://doi.org/10.1007/s12599-022-00783-7

Kompaniets, A., & Chemerys, H. (2019). Generalization of the experience of using research on psychology of behavior for designing UX design software products. *Ukrainian Journal of Educational Studies and Information Technology*, *7*(3), 1-10. https://doi.org/10.32919/uesit.2019.03.01

Krauß, V., Saeghe, P., Boden, A., Khamis, M., McGill, M., Gugenheimer, J., & Nebeling, M. (2024). What Makes XR Dark? Examining Emerging Dark Patterns in Augmented and Virtual Reality through Expert Co-Design. *ACM Trans. Comput.-Hum. Interact.*, *31*(3), Article 32. https://doi.org/10.1145/3660340

Krisam, C., Dietmann, H., Volkamer, M., & Kulyk, O. (2021). Dark Patterns in the Wild: Review of Cookie Disclaimer Designs on Top 500 German Websites. *Proceedings of the 2021 European Symposium on Usable Security, Karlsruhe, Germany.* https://doi.org/10.1145/3481357.3481516

Lachheb, A., Abramenka-Lachheb, V., Moore, S., & Gray, C. (2023). The role of design ethics in maintaining students' privacy: A call to action to learning designers in higher education. *British Journal of Educational Technology*, *54*(6), 1653-1670. https://doi.org/https://doi.org/10.1111/bjet.13382

Leiser, M. R., Kosta, E., Leenes, R., & Kamara, I. (2022). Chapter 10: Dark patterns: The case for regulatory pluralism between the European Unions consumer and data protection regimes. In E. Kosta, R. Leenes, & I. Kamara (Eds.), *Research Handbook on EU Data Protection Law* (pp. 240-269). Edward Elgar Publishing. https://doi.org/10.4337/9781800371682.00019

Lu, Y., Zhang, C., Yang, Y., Yao, Y., & Li, T. J.-J. (2024). From Awareness to Action: Exploring End-User Empowerment Interventions for Dark Patterns in UX. *Proc. ACM Hum.-Comput. Interact.*, *8*(CSCW1), Article 59. https://doi.org/10.1145/3637336

Luguri, J., & Strahilevitz, L. J. (2021). Shining a Light on Dark Patterns. *Journal of Legal Analysis*, *13*(1), 43-109. https://doi.org/10.1093/jla/laaa006

Machuletz, D., & Böhme, R. (2020). Multiple purposes, multiple problems: A user study of consent dialogs after GDPR. *Privacy Enhancing Technologies,* https://doi.org/10.2478/popets-2020-0037

Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. *Proc. ACM Hum.-Comput. Interact.*, *3*(CSCW), Article 81. https://doi.org/10.1145/3359183

Mathur, A., Kshirsagar, M., & Mayer, J. (2021). What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, Yokohama, Japan.* https://doi.org/10.1145/3411764.3445610

Naslund, J. A., Aschbrenner, K. A., Kim, S. J., McHugo, G. J., Unützer, J., Bartels, S. J., & Marsch, L. A. (2017). Health behavior models for informing digital technology interventions for individuals with mental illness. *Psychiatr Rehabil J*, *40*(3), 325-335. https://doi.org/10.1037/prj0000246

Nazarov, D., & Baimukhambetov, Y. (2022). Clustering of Dark Patterns in the User Interfaces of Websites and Online Trading Portals (E-Commerce). *Mathematics*, *10*(18), 3219. https://doi.org/10.3390/math10183219

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, Honolulu, HI, USA*. https://doi.org/10.1145/3313831.3376321

Radesky, J., Hiniker, A., McLaren, C., Akgun, E., Schaller, A., Weeks, H. M., Campbell, S., & Gearhardt, A. N. (2022). Prevalence and Characteristics of Manipulative Design in Mobile Applications Used by Children. *JAMA Network Open*, *5*(6), e2217641-e2217641. https://doi.org/10.1001/jamanetworkopen.2022.17641

Sin, R., Harris, T., Nilsson, S., & Beck, T. (2025). Dark patterns in online shopping: do they work and can nudges help mitigate impulse buying? *Behavioural Public Policy*, *9*(1), 61-87. https://doi.org/10.1017/bpp.2022.11

Singh, V., Vishvakarma, N. K., & Kumar, V. (2024). Unmasking user vulnerability: investigating the barriers to overcoming dark patterns in e-commerce using TISM and MICMAC analysis. *Journal of Information, Communication and Ethics in Society*, *22*(2), 275-292. https://doi.org/10.1108/JICES-10-2023-0127

Singh, V., Vishvakarma, N. K., & Kumar, V. (2025). Profit over principles: unveiling the motivating factors behind dark patterns in e-commerce through the lens of agency theory. *Journal of Enterprise Information Management*, *38*(3), 821-848. https://doi.org/10.1108/JEIM-08-2024-0409

van Nimwegen, C., Bergman, K., & Akdag, A. (2022, July, 11-13). Shedding light on assessing Dark Patterns: Introducing the System Darkness Scale (SDS). *35th International BCS Human-Computer Interaction Conference (HCI2022), Keele, Staffordshire.* https://doi.org/10.14236/ewic/HCI2022.7

Voigt, C., Schlögl, S., & Groth, A. (2021, 07/24-29). Dark Patterns in Online Shopping: of Sneaky Tricks, Perceived Annoyance and Respective Brand Trust. *HCI in Business, Government and Organizations, Cham*. https://doi.org/10.1007/978-3-030-77750-0_10

White, C. (2015). The impact of motivation on customer satisfaction formation: a self-determination perspective. *European Journal of Marketing*, *49*(11/12), 1923-1940. https://doi.org/10.1108/EJM-08-2014-0501

Zagal, J. P., Björk, S., & Lewis, C. (2013, May 14-17). Dark patterns in the design of games. International Conference on Foundations of Digital Games, Chania, Crete, Greece.

Zhang, K., & Gao, Y. (2022, 2022/11/19). Analysis of Research Hotspots of Cognitive Load from the Perspective of Product Design Based on Measurement System, Cause Analysis, and Regulation Strategy. *Proceedings of the 2022 International Conference on Science Education and Art Appreciation (SEAA 2022)*, https://doi.org/10.2991/978-2-494069-05-3_80