Addressing the regulatory gaps in the dark patterns in online platforms (Checkpoint 4)

Hasara Kalumin* Ritesh Kumar Das† Allen Sunny‡

December 10, 2024

1 Introduction

Prior studies have shown that individual preferences are subjective to framing effects[1] and different behaviors can be observed in the same setting by just altering the framing of the situation. Similarly, research suggests that individuals resort to certain heuristics in making decisions and this potentially leads to inherent cognitive biases[2] which can be exploited to direct individual behavior in specific directions. Research on individual behavior in online platforms provides credence to these theories. Framing of choices can significantly impact users' online purchase decisions[3]. Manipulations of choice frames in the context of online privacy can also significantly influence the privacy choices of the users[4]. Moreover, consumers are likely to overestimate their response to normative factors and underestimate their response to behavioral factors in privacy decision-making[4]. Consumer decisions at the time of consumption are also impacted by the predictions generated by recommender systems and the ratings provided by recommender systems serve as an anchor for the consumer's constructed preferences [5]. This has subsequently led to the phenomenon referred to as dark patterns [6]), user interface design elements that

*Department of Computer Science, University of Maryland
†Robert H. Smith School of Business, University of Maryland
‡College of Information, University of Maryland

benefit organizations by deceiving and manipulating users [7],[8]. These infringe on user autonomy by preventing user choices [9], [10].

In the context of online systems, user autonomy can be defined as self-governance that leads to independent choices and the expression of free will among users[11]. However, user choices are subject to a host of cognitive heuristics and biases, especially in online platforms which can be exploited to channel their behavior towards desired outcomes. This calls for explicit regulations to ensure consumers are protected from these deceptive design techniques. This study tries to review the existing literature on the latest regulations on dark patterns, identify potential gaps, and suggest possible measures.

2 Dark Patterns

"Dark patterns" refer to user interface designs that are crafted to manipulate or deceive users into making decisions they would not otherwise make. Coined by [6], dark patterns exploit cognitive biases and vulnerabilities, steering users towards choices that benefit the designer's goals, often at the expense of the user's interests. These manipulative techniques are prevalent in digital environments such as websites, mobile apps, and online shopping platforms, raising concerns among scholars and consumer protection advocates alike. [6]'s foundational work classified dark patterns into various categories, including hidden costs, bait and switch, forced continuity, and privacy zuckering [6]. These design techniques aim to increase engagement or revenue by subtly manipulating user behavior. [12] expanded on this by categorizing dark patterns into five main types: asymmetry, covert, deceptive, restrictive, and skewed choices, arguing that such designs often obfuscate the consequences of users' actions. The ethical implications of dark patterns have been widely discussed, particularly in terms of user autonomy and informed consent.[13] emphasized that dark patterns undermine ethical design principles by prioritizing corporate profits over user welfare. They argue that such designs exploit users' cognitive limitations, making it difficult for them to make informed decisions. From a psychological perspective, dark patterns manipulate common human cognitive biases such as the

endowment effect, loss aversion, and social proof. [14] explored how manipulative designs capitalize on these biases, encouraging impulsive actions or compliance. For instance, pre-checked boxes in online shopping encourage users to purchase additional services by leveraging inattention and default bias.

A substantial body of empirical research has explored the prevalence of dark patterns. [12] conducted a large-scale study of over 11,000 shopping websites, identifying more than 1,800 instances of dark patterns. Their research found that deceptive patterns are most commonly associated with e-commerce platforms that rely on sales conversion tactics, such as countdown timers, limited-time offers, and forced enrollment in subscription services. Based on this study, the researchers defined a taxonomy of dark pattern characteristics which contains the following dimensions:

- Asymmetric: The UI design focuses more on particular choices compared to others.
- Covert: The design tries to distract the user and steer them into making an unintended decision.
- Deceptive: The design can encourage false beliefs by using affirmative, misleading statements or omissions.
- Hides information: The user interface might obscure or delay the presentation of key information.
- Restrictive: The UI design can limit the number of choices presented to users.

Therefore, through exploiting users' cognitive biases, dark patterns have been able to manipulate users into making unintended decisions that can be potentially harmful in the long term. Similarly, [15] analyzed how social media platforms employ dark patterns to retain users. They identified manipulative tactics such as infinite scrolling, personalized notifications, and obfuscated privacy settings, which compel users to spend more time on the platform or unwittingly disclose personal information. [16] gives very detailed manifestation techniques of dark patterns commonly observed in digital platforms, they can be summarized below-

- Misdirection techniques- using visuals or language to direct users away from a choice.

- Confirm shaming techniques- presenting users with negatively framed decline options.
- Framing techniques- focusing wording around the positive aspects of a choice and glossing over the negative consequences of a choice.
- Obstruction techniques- making it extremely easy to sign up but incredibly difficult to cancel a membership or subscription.
- Nagging techniques- involves pop-up messages or interruptions that force users to make a choice, and often interrupt the activities and browsing flow of users.
- Fake notification techniques- using interfaces indicating that users have received messages or notifications that do not exist.
- Disguised advertising techniques- advertisers displaying materials amid the content of other websites/pages.
- Scarcity techniques- an online service provider indicating artificial scarcity to create a sense of urgency for the user to complete their purchase.
- Preventing price comparisons techniques- websites make it difficult to compare the prices of various products or services offered on their platform.
- Trick question techniques- intentionally worded, framed, or ordered questions to trick users into providing an answer or selecting an option they did not intend to.
- Friend spam techniques- using users' emails or social media permissions to automatically send messages to people in their contact lists appearing as the user.
- Default setting techniques- setting the default at the maximum level of data sharing or the most privacy-intrusive option.
- Inertia selling techniques- adding items automatically to a user's shopping cart
- Forced action techniques- forcing users to perform a certain action to access or continue accessing a function on a platform.

As dark patterns have garnered more attention, they have become the subject of legal scrutiny. From the regulatory point of view, there must be checks and balances on each of the techniques listed above, including their subtle modifications. Laws like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) have provisions intended to curtail the use of deceptive interfaces, particularly concerning

privacy settings and data consent mechanisms. [17] conducted experiments on the impact of dark patterns in privacy decision-making and argued that the legal frameworks need to explicitly address these designs to ensure consumer protection.

3 Stakeholders

Regulating dark patterns on the internet has become increasingly crucial, especially as their prevalence has surged in an unregulated environment, as highlighted by recent studies [18], [19]. Evidence shows that end users are losing money in various ways, such as overpaying on taxes [20], incurring additional costs for subscriptions [4], or having their data leaked for targeted advertising[21]. In this landscape of dark patterns, stakeholders can be broadly categorized into four distinct groups.

The end users are the most critical stakeholders in the context of dark patterns. Recent legal activity such as the GDPR[22] and the CCPA [23], affirm that users have the right to engage with digital services without manipulation from the companies that provide them. Additionally, emerging legal frameworks like the EU AI Act [24], offer more robust protections against dark patterns, further reinforcing users' rights and ensuring a safer digital environment. Understanding how users interact with dark patterns is essential for assessing their impact on decision-making, trust, and overall satisfaction. User studies, such as [25], have traced user behavior patterns, illustrating how they are influenced by these manipulative tactics. Understanding how users interact with a website is paramount in creating enforceable systems.

Designers and the companies they work for play a vital role in this ecosystem. Driven by metrics like conversion rates and user engagement, designers may unintentionally implement manipulative tactics due to pressure to meet specific goals [26]. Critical and reflexive design approaches have emerged as responses to these pressures [27],[28], along with value-sensitive design [29] and persuasive design[14], which advocate for more ethical practices. Other ethically driven design principles that highlight dual privacy, disclosure, accuracy, and the "golden" principle [30] have started to take hold as a pushback against

company pressure. While companies may implement dark patterns to maximize profits, such strategies can ultimately harm the brand reputation and erode consumer trust. [31] As awareness of these practices grows, companies face increasing scrutiny from consumers and regulators, necessitating a shift towards more responsible design practices. This of course cannot happen without a robust regulatory framework and public awareness of predatory design practices. Governmental organizations and regulators represent the third pillar in the discussion surrounding dark patterns. They hold the authority to establish rules and regulations that can modify website designs to mitigate the harmful effects of these manipulative tactics. There is a growing consensus that users should not be subjected to digital manipulation; however, the regulatory landscape is still evolving, and many enforcement mechanisms and other critical aspects remain to be fully defined.[26]

Governments have a vested interest in regulating dark patterns to ensure fair market practices [32] and foster consumer trust [33], which ultimately contributes to a healthier business environment. For instance, regulatory frameworks like the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States provide foundational protections against manipulative practices, promoting transparency and accountability among companies. Additionally, the proposed EU AI Act aims to establish further safeguards against the misuse of artificial intelligence, reinforcing the necessity for ethical design in digital products. As public awareness of dark patterns increases, the pressure on regulators to take action also grows. By enacting and enforcing regulations, governments can protect consumers from deceptive practices [34], ensuring that the digital landscape remains equitable and fair. This not only helps in safeguarding individual rights but also promotes competition and innovation within the market. In this way, effective regulation can lead to a more trustworthy digital environment, ultimately benefiting both consumers and businesses alike.[35]

The final group consists of extra-governmental entities, including media, watchdog organizations, and academics. The media plays a crucial role as a watchdog and educator regarding dark patterns.[36] By investigating and reporting on manipulative design practices, media outlets help raise public awareness and inform consumers about their

rights. Investigative journalism can expose unethical practices, prompting public outrage and influencing regulatory discussions. Watchdog organizations, such as consumer rights groups and digital rights advocates [37], actively monitor company practices concerning dark patterns. They conduct research and publish reports on the prevalence and impact of these manipulative designs, advocating for stronger regulations and ethical standards. Ethicists and academics contribute to the dialogue surrounding dark patterns by analyzing the moral implications of design choices. They explore issues related to user autonomy and informed consent, engaging with businesses and regulatory bodies to promote ethical design principles that respect individual rights. This collective effort among stakeholders is essential for addressing the challenges posed by dark patterns and ensuring a fairer digital landscape for all users.

4 Existing Legal and Regulatory Measures on Dark Patterns

The General Data Protection Regulation (GDPR), which came into effect in 2018 in the European Union, is one of the most significant legal frameworks addressing digital manipulation, including dark patterns. The GDPR aims to protect user autonomy in data processing and requires explicit, informed consent for data collection and use. Several provisions within the regulation target dark patterns:

- Consent Mechanisms: Under GDPR, consent must be "freely given, specific, informed, and unambiguous" (Article 4(11)). Dark patterns such as pre-checked boxes for consent or buried terms of service that obfuscate privacy policies are considered violations of this principle.
- Right to Withdraw Consent: GDPR enforces that users must be able to withdraw consent as easily as they gave it (Article 7). This aspect directly counters designs that make opting out of services or subscriptions difficult (e.g., forced continuity).

Studies such as the work by [38] argue that GDPR has made strides in curbing certain dark patterns, especially in data collection, but it has limitations. Violations are often

difficult to enforce, especially with large multinational companies that obscure the consent process across jurisdictions. [39] noted that while GDPR provides a strong foundation for addressing dark patterns, enforcement authorities across EU member states need to take a more active role in ensuring compliance.

The California Consumer Privacy Act (CCPA), enacted in 2020, is another key regulatory framework targeting dark patterns, particularly in data privacy and consumer consent. The CCPA gives California residents the right to know what personal data is being collected, the right to delete data and the right to opt out of data sales. However, concerns over dark patterns led to the introduction of the California Privacy Rights Act (CPRA), which strengthens certain provisions of the CCPA. Opt-Out Mechanisms: Under the CCPA and CPRA, dark patterns that complicate or mislead users into staying enrolled in data collection or selling processes are prohibited. The CPRA defines "dark patterns" explicitly as designs that "have the substantial effect of subverting or impairing user autonomy, decision making, or choice" (CPRA, Section 1798.140(l)). Informed Consent: The CPRA builds on the CCPA by requiring that consent be freely given, informed, and specific, echoing the GDPR's provisions.

[17] tested the effectiveness of these laws, finding that while CCPA and CPRA target harmful patterns, the language in these laws remains broad, leaving room for exploitation. They argue that more specific guidelines for dark patterns are needed to ensure full protection. In the United States, the Federal Trade Commission (FTC) plays a crucial role in addressing dark patterns under its authority to regulate unfair and deceptive trade practices. Although no specific federal law is aimed solely at dark patterns, the FTC's Section 5 of the FTC Act (15 U.S.C. - 45) prohibits "unfair or deceptive acts or practices in or affecting commerce." The FTC has started applying this statute to deceptive digital practices.

- Deceptive Designs in Commerce: The FTC has issued warnings and fines to companies employing dark patterns in areas such as e-commerce (e.g., subscription traps), misleading advertising, and privacy violations. The FTC's 2021 Dark Patterns Workshop aimed to raise awareness of the tactics that deceive or manipulate

users and highlight enforcement priorities.

- Recent Enforcement Actions: In 2021, the FTC settled cases against several companies for using dark patterns to mislead consumers into subscription services. These actions reflect the growing interest in holding companies accountable for designs that obfuscate cancellation options or hide additional costs.

However, [25] notes that while the FTC has the authority to act against dark patterns, it lacks the resources to pursue all violators comprehensively. Moreover, the absence of specific federal laws targeting dark patterns means enforcement remains piecemeal, relying on the broad interpretation of deceptive practices. Several digital platforms and app marketplaces have introduced self-regulatory measures to combat dark patterns. For instance, Apple's App Store and Google Play have established guidelines requiring transparency in in-app purchases, subscription services, and user permissions.

- App Store Guidelines: Apple introduced policies in 2020 aimed at reducing dark patterns, particularly those involving misleading subscription practices. Developers are required to present clear, upfront information about pricing and cancellation policies.

- Google Play Policies: Google Play also updated its guidelines to require apps to make opt-out and cancellation mechanisms easily accessible to users. Moreover, apps that exploit users through deceptive designs can be removed from the marketplace.

[12] argues that while self-regulation has helped reduce some instances of dark patterns, it often lacks the enforcement mechanisms and penalties needed to deter large companies from using manipulative designs. They recommend stronger legislative frameworks alongside self-regulation to ensure consistency across digital platforms.

Despite these laws and regulations, several challenges remain in effectively regulating dark patterns. First, vague legal definitions of what constitutes a dark pattern make enforcement difficult. As [25] points out, without clear, consistent definitions across legal frameworks, many companies continue to exploit loopholes. Second, the global nature of

digital commerce complicates enforcement, as companies operating across borders may fall under different jurisdictions, each with varying levels of regulation. Finally, consumer awareness and education are crucial in combating dark patterns. [40] suggests that legal frameworks should not only target companies but also promote transparency and education for consumers to recognize manipulative designs. This could be achieved through clearer labeling, public awareness campaigns, or user tools that highlight dark patterns.

5 Regulatory Gaps

The legal response to dark patterns operates along two primary axes: **regulation** and **enforcement**. These vary significantly across countries, with both the existence of regulations and the degree of enforcement differing widely.

The metrics for regulation and enforcement follow a **High/Medium/Low** scale:

- **Regulation:** Assessed based on whether a regulation is explicitly crafted for a particular dark pattern technique (**High**), if existing regulations can be adapted to cover the technique (**Medium**), or if no regulations address it (**Low**).
- **Enforcement:** Evaluated by the frequency of citations by relevant agencies—**High** if cited over five times, **Medium** if cited 1-5 times, and **Low** if not cited at all.

The table below summarizes the current status of regulations and enforcement for each technique of dark patterns considered by us.

Dark Patterns and Relevant Regulations

Regulation	Description	Regulation vs Enforcement
Framing		
Federal Trade Commission (FTC) [41]	The FTC's Enforcement Policy Statement on Deceptively Formatted Advertisements requires that advertising must not mislead consumers.	Medium Regulation vs. Medium Enforcement
CCPA [42] and CPRA[43]	These acts include consent and opt-out provisions.	Medium Regulation vs. Low Enforcement
Proposed DETOUR Act[44]	The proposed DETOUR Act targets dark patterns designed to coerce or deceive users.	Proposed Regulation
Obstruction		
FTC's Click-to-Cancel Rule[41]	The rule mandates straightforward cancellation processes to prevent obstructive tactics in subscriptions.	High Regulation vs. Medium Enforcement
CCPA [42]	CCPA mandates ease of opting out of data sales and deleting personal data.	High Regulation vs. Medium Enforcement
Forced Continuity		
FTC's Click-to-Cancel Rule [41]	Requires companies to offer straightforward cancellation methods for subscriptions.	High Regulation vs. Low Enforcement
California Automatic Renewal Law (ARL)[45]	Mandates disclosure of auto-renewal terms and easy cancellation.	High Regulation vs. Low Enforcement

Regulation	Description	Regulation vs Enforcement
Unsubscribe Act (To be passed) [46]	Expand regulation on automatic renewals by requiring clear notifications, consent before billing etc	Low Regulation vs. Low Enforcement
Nagging		
CCPA [42]	Under the CCPA, businesses must provide clear opt-out options for data sharing. Repeated consent requests can be seen as coercive, potentially violating provisions if they pressurize users into compliance.	Medium Regulation vs. Low Enforcement
FTC's Focus on Dark Patterns[47]	The FTC has highlighted dark patterns like nagging that interfere with consumer autonomy. The agency warns that repeated prompts, such as those for accepting terms or consenting to tracking, could be considered deceptive.	High Regulation vs. Low Enforcement
Fake Notifications		
FTC Guidelines on Deceptive Practices[47]	The FTC prohibits deceptive practices, with fake notifications falling under this if they mislead users into unwanted decisions.	High Regulation vs. High Enforcement
Scarcity		
FTC[47]	Prohibits false scarcity claims that mislead consumers, with recent actions against misleading countdowns.	Medium Regulation vs. Low Enforcement
Friend Spam		

Regulation	Description	Regulation vs Enforcement
CAN-SPAM Act[48]	Requires clear opt-out options for email marketing, though friend spam operates in a gray area.	Medium Regulation vs. Medium Enforcement
CCPA [42]	Provides users control over data sharing, relevant for apps using contact lists for unsolicited messages.	High Regulation vs. Low Enforcement
Inertia Selling		
FTC Regulations[47]	Prohibits demanding payment for unsolicited items, which consumers can keep without obligation.	High Regulation vs. Medium Enforcement
Forced Action		
CCPA [42]	CCPA gives users data control, potentially conflicting with forced data-sharing requirements.	Medium Regulation vs. Medium Enforcement
FTC [47]	Discourages coercive actions that push users into unwanted agreements.	Low Regulation vs. Low Enforcement
Price Comparison Prevention		
Robinson-Patman Act [49]	Prohibits price discrimination but is limited to wholesale and retail, excluding individual consumers.	Low Regulation vs. Low Enforcement

Also, we analyze the major regulatory acts in the following 7 dimensions:

- scope
- Proactive detection
- Technological integration
- Adaptability - Adaptability to emerging dark patterns
- User empowerment - Giving control to users and ensuring transparency, accessibil-

ity, and fairness

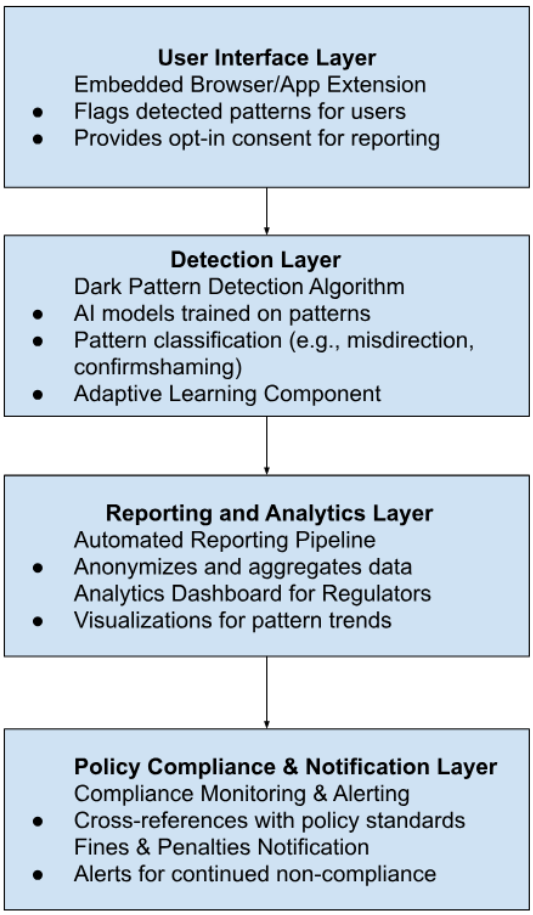
- Enforcement speed
- Educational component - Educating users through the regulations

Feature	**GDPR**	**FTC Act**	**CCPA**	**COPPA**	**CMA(UK) Act**
Scope	Data privacy	Broad but unfocused	Data Privacy	Children focused	Lacks comprehensive framework
Proactive Detection	No	No	No	No	No
Technological Integration	None	None	None	None	None
Adaptability	Limited	Limited	Limited	Static (rely on predefined rules)	Static
User Empowerment	Indirect	Indirect	Indirect	Indirect	Indirect
Enforcement Speed	Slow (audits)	Slow	Complaint based	Complaint based	Case-by-case
Educational Component	No	No	No	No	No

6 Proposed Intervention - Regulatory Technology tool

A comprehensive solution to address dark patterns through both policy intervention and technology could involve a Dark Pattern Detection and Reporting System embedded in web browsers, apps, and operating systems. This system would not only identify and flag dark patterns in real time but also collect data for regulatory agencies, which could enforce compliance based on these patterns. This system can act as a regulatory tool, providing a systematic approach to regulating dark patterns while complying with existing regulations.

Figure 1: System Architecture



6.1 Dark Pattern Detection and Reporting System - Browser/App Extension to detect dark patterns

Key Components of the System

- User Interface (UI) Layer
  - Embedded in Browsers and Apps: A browser extension, app integration, or operating system feature flags dark patterns and issues real-time warnings to users. This UI layer provides a simple, intuitive way to notify users of potential manipulation.
  - Opt-In Consent for Data Collection: Users are informed about data collection for regulatory oversight and can opt-in to anonymously report instances where they encounter dark patterns.

- Detection Layer (AI-Powered)
  - Dark Pattern Detection Algorithm: An AI model trained on a library of known dark patterns, continuously updated by regulatory agencies, developers, and open-source contributors.
  - Pattern Classification System: This system categorizes detected patterns as misdirection, confirm-shaming, framing, etc., providing context for the user and storing data for regulatory review.
  - Adaptive Learning Component: A machine learning feature that adapts as new patterns emerge. Regulatory bodies or trusted entities would train this model on updates, ensuring it reflects evolving manipulative tactics.
- Reporting and Analytics Layer
  - Automated Reporting Pipeline: Aggregates and anonymizes flagged data points and compiles reports for regulators. This data pipeline ensures user privacy while providing high-level insights on dark patterns across industries.
  - Analytics Dashboard for Regulators: Regulatory agencies access a dashboard that shows dark pattern trends by company, industry, and type. This allows agencies to pinpoint persistent offenders and trends that require policy updates.
- Policy Compliance and Notification Layer
  - Compliance Monitoring and Alerting System: Tracks flagged instances by companies and cross-references them with legal standards (GDPR, CCPA, DSA, etc.). Companies receive warnings or notifications to adjust their practices when detected patterns violate policy.
  - Fines and Penalties Notification: Automatically triggers warnings or notifications to companies in cases of continued non-compliance, aligning enforcement with existing legal frameworks.

System workflow

- Real-Time Detection and Classification
  - When a user interacts with a potentially deceptive interface, the Detection Layer activates, scanning for elements that match patterns of misdirection, confirmshaming, or framing. This may include hidden or obscured unsubscribe links, guilt-inducing language, or misleading button placement.
  - The algorithm then classifies the pattern type and displays a notification to the user, highlighting elements in the UI that are potentially deceptive.
- User Reporting and Feedback
  - Users can report instances that seem deceptive directly through the UI. If they opt-in, these instances are anonymized and logged in the Reporting Layer. Reports provide invaluable feedback to improve the algorithm and allow agencies to prioritize oversight based on real user experiences.
- Policy Compliance Monitoring
  - The Compliance and Notification Layer cross-references detected dark patterns against existing regulations. For instance, if a website consistently uses confirm shaming tactics, this would be flagged and recorded.
  - Repeat offenders can be reported to regulatory agencies, with penalties issued in line with existing laws, thus creating a direct link between dark pattern detection and legal enforcement.
- Adaptive Learning and Regulatory Insights
  - Using data collected from reports and real-time detections, regulatory bodies receive trend analysis of common dark patterns, allowing them to stay updated on evolving practices.

– The adaptive learning component can incorporate new pattern types, ensuring that detection capabilities grow alongside shifts in online manipulation techniques.

This technology integration could help ensure that online services adhere to ethical standards while minimizing the manipulation of users through dark patterns. This solution addresses the dark patterns problem from multiple angles—empowering consumers, equipping regulators, and enforcing compliance—all with the help of advanced, adaptive technology. Unlike existing approaches, which are mostly regulatory or reactive in nature, this proposal combines existing regulations and policy standards with a scalable technological intervention that operates across platforms. The adaptive learning model is especially novel, as it provides a forward-looking, flexible solution that evolves in tandem with dark patterns, while also harnessing regulatory oversight through real-time insights.

Ultimately, this approach represents a proactive shift in policy, integrating cutting-edge technology to address a modern digital problem, rather than relying solely on traditional legal frameworks that are less agile. This fusion of policy and technology could set a new precedent for tackling other digital consumer protection issues, potentially paving the way for similar models in areas like misinformation, cyberbullying, and online fraud.

6.2 Benefits, novelty, barriers, and costs for proposed interventions

6.2.1 Benefits of the solution

- Transparency for Users: Real-time detection helps users make informed choices and builds trust in digital services.
- Data-Driven Enforcement: Regulatory agencies receive reliable data on dark pattern usage, helping them to target the worst offenders.
- Industry Accountability: Automated compliance checks and alerts push companies toward ethical practices, reducing the prevalence of dark patterns.

6.2.2 Comparison of the novelty of the solution to existing interventions for dark patterns

We focus on the key elements such as scope, enforcement mechanisms, technological integration, and flexibility.

Feature	Proposed Intervention
Scope	Comprehensive: All dark patterns
Proactive Detection	Real-time AI-driven detection
Technological Integration	Mandates detection/reporting tools
Adaptability	Adaptive AI new dark patterns
User Empowerment	Notifications+transparency
Enforcement Speed	Proactive and automated enforcement
Educational Component	Educates users on dark patterns

Table 2: Proposed intervention addressing the existing gaps

1. California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)

   Overview: CCPA and CPRA regulate data privacy and consent, requiring companies to disclose data collection practices, give consumers the right to opt out, and protect minors from targeted advertising.

   Comparison: The CCPA/CPRA focus on data privacy, particularly the rights to access, delete, and opt-out of data sharing. They do not specifically address dark patterns but do restrict "deceptive" consent practices that can be considered as dark patterns. Enforcement is reactive, relying on penalties for non-compliance rather than actively detecting dark patterns. The CCPA and CPRA do not mandate any specific technology for compliance or detection; instead, they focus on policy-level regulations, which leave room for businesses to interpret the rules. CCPA/CPRA lack adaptability in tracking dark patterns. While the law can penalize deceptive practices, it doesn't actively evolve to recognize new manipulative designs as they emerge.

   Novelty of Proposed Solution: The proposed solution goes beyond data consent to detect and report manipulative UI elements in real-time, proactively preventing

dark patterns across various contexts. Unlike CCPA, it actively integrates adaptive learning algorithms to track evolving dark patterns, which CCPA lacks.

2. European Union's General Data Protection Regulation (GDPR)

   Overview: GDPR governs data processing and consent, establishing stringent requirements for clear and informed consent from users. It emphasizes transparency and prohibits deceptive data collection practices, indirectly affecting certain dark patterns.

   Comparison: GDPR focuses on data privacy and requires companies to obtain "freely given, specific, informed, and unambiguous" consent, which indirectly limits certain dark patterns like "forced consent" but does not directly address UI manipulations outside consent. GDPR relies on data protection authorities (DPAs) and consumer complaints to enforce regulations, making it reactive rather than proactive in dark pattern detection. GDPR lacks specific technology mandates for detecting dark patterns; it relies on company compliance audits and DPA oversight. It has broad definitions around consent but lacks the capability to adapt to specific emerging dark patterns, which makes enforcement on design-specific issues challenging.

   Novelty of Proposed Solution: The proposed intervention would add technological solutions for continuous detection and compliance monitoring, going beyond GDPR's indirect influence on dark patterns. The adaptive learning and real-time user notification elements are distinct, making this proposal more effective at catching patterns as they evolve.

3. DETOUR Act (Deceptive Experiences To Online Users Reduction Act)

   Overview: The DETOUR Act, proposed in the U.S. Senate, targets deceptive and manipulative practices by large online platforms, specifically focusing on user consent manipulation, such as confirm shaming or misdirection.

   Comparison: The DETOUR Act directly addresses manipulative design practices by requiring large platforms to disclose manipulative strategies and prevent tactics

that coerce users. The Act relies on FTC oversight and imposes fines on platforms using dark patterns, particularly those that influence addictive behaviors and data consent manipulation. However, enforcement largely depends on regulatory monitoring and complaints. The DETOUR Act does not propose any AI-based or real-time detection technology, instead focusing on oversight through reporting and compliance requirements. The Act mandates transparency and disclosures but lacks provisions for dynamically adapting to new dark patterns, which could allow companies to bypass its rules with emerging tactics.

Novelty of Proposed Solution: The proposed solution's technological approach with real-time detection and adaptive learning provides an automated and proactive monitoring layer that DETOUR lacks. Instead of relying solely on regulatory intervention, it incorporates AI to flag patterns in real-time, which could reduce regulatory lag and improve enforcement.

4. Federal Trade Commission (FTC) Act and FTC Enforcement

   Overview: The FTC Act allows the FTC to address "unfair or deceptive practices" broadly, which includes enforcing penalties against companies for deceptive user interface designs as part of its consumer protection mandate.

   Comparison: The FTC can take action against dark patterns as deceptive practices but is limited to post-hoc investigations and consumer complaints. The FTC's enforcement is largely complaint-driven and reactive, often responding to significant complaints or trends rather than monitoring individual manipulations in real-time. The FTC relies on human-driven investigations, audits, and regulatory action without technological solutions for dark pattern detection. Without specific regulations targeting dark patterns, the FTC's actions are inconsistent and vary case by case, which limits its ability to address the nuanced aspects of UI manipulations.

   Novelty of Proposed Solution: The proposed solution offers a systematic, technology-driven policy that proactively monitors dark patterns, reducing dependency on consumer complaints. By using AI and real-time detection, it would enable a more

efficient and consistent regulatory response compared to the current reactive model.

Our solution stands out due to its focus on technological enforcement rather than solely relying on broad legal standards, as seen in most existing laws. By proposing a real-time, AI-driven detection and reporting system, this solution shifts from the traditional regulatory approach to a proactive, preventative measure that directly mitigates manipulative design tactics as they occur. Additionally, the adaptive learning model makes this solution future-proof, allowing it to respond to new dark patterns faster than regulatory updates alone. In essence, this proposal fills a gap by combining automated enforcement, user empowerment, and regulatory transparency in a way that existing policies do not, setting a new benchmark for handling digital manipulations dynamically and at scale.

6.2.3 Does the scientific research community have sufficient knowledge to enact on this proposed solution, or is more research required?

1. Understanding of Dark Patterns: Research has extensively cataloged dark patterns, identifying common manipulative tactics like misdirection, confirm-shaming, and forced continuity. Studies categorize these patterns by intent and effect, providing an important baseline for policy and automated detection.

2. Machine Learning for Dark Pattern Detection: Techniques for automated UI analysis and machine learning (ML) have progressed significantly. Studies have explored natural language processing (NLP) and computer vision to identify manipulative language or misleading visuals within interfaces. These models can detect simple patterns effectively, and ongoing research continues to enhance their ability to generalize across platforms.

3. Ethics and Human-Centered AI: Researchers have developed ethical guidelines for AI in consumer protection, focusing on transparency, explainability, and user agency. This helps ensure that any real-time notification system for dark patterns respects user privacy and ethical AI principles, which are vital for the DPDRS solution.

4. Adaptive Algorithms and Consumer Privacy: Adaptive learning, especially in recommender systems, is well-researched and relevant to this solution. Privacy-preserving ML techniques like differential privacy and federated learning are being refined, helping the proposed solution balance effectiveness with privacy needs.

Here we list the areas that we believe should be further investigated.

1. Generalization Across Diverse Platforms and Dark Patterns: Detecting dark patterns in varied contexts and interfaces across e-commerce, social media, gaming, etc. remains a challenge. While detection models are effective for some patterns (e.g., forced continuity), others (e.g., emotional manipulation or nuanced framing) may evade current algorithms. Generalizing models to work across sectors with diverse patterns requires additional research in both interface analysis and contextual ML.

2. Real-Time Detection with Low False Positives: Real-time, high-accuracy dark pattern detection is complex. The user notification system must avoid overwhelming users with alerts, as frequent false positives could lead to alert fatigue. Research to improve real-time detection accuracy while minimizing false positives is crucial, especially for dynamic websites and apps where content changes frequently.

3. Effectiveness of User Notification and Engagement: The psychological impact and usability of real-time notifications are not fully understood. Over-notifying or misjudging dark patterns may backfire, diminishing user trust in the system. More research is needed to optimize notification strategies—testing timing, language, and interface to maximize user engagement without causing annoyance or fatigue.

4. Adapting Detection Models to New and Evolving Dark Patterns: Dark patterns are rapidly evolving, and existing detection models can struggle with new tactics, not in their training data. Research into adaptive machine learning models that update continuously without extensive retraining could be key to keeping up with manipulative techniques as they emerge.

5. Data Privacy and Security in Anonymized Pattern Reporting: While anonymization techniques are well-studied, implementing them in a way that maintains high security and privacy in real-time detection systems still requires more research. Effective anonymization that balances data utility for regulators with strong user privacy is crucial, especially as pattern reporting expands across different sectors and interfaces.

6. Regulatory Integration and Standards for Dark Pattern Detection: Research is needed to establish standardized metrics for measuring dark patterns across platforms and applications. Regulatory bodies would benefit from clear, uniform criteria to evaluate manipulative practices, and further research could help create actionable standards that support the technological solution.

While the foundational knowledge exists, further research is needed to refine aspects of real-time detection, user engagement, adaptive learning, and privacy-preserving data collection. Key areas like notification impact, adaptive algorithms for new dark patterns, and regulatory standards would benefit from deeper exploration to ensure the solution is effective and scalable.

6.2.4 Barriers to the proposed solution

While the proposed Dark Pattern Prevention and Consumer Protection Act seeks to address a growing problem in consumer protection, it faces significant barriers from a technological, financial, regulatory, and social perspective. Several powerful stakeholders, including e-commerce companies, advertising agencies, and tech giants, have a vested interest in opposing it due to potential impacts on their revenue, business models, and operational flexibility. To overcome these barriers, the proposal would need a phased approach with stakeholder engagement, privacy protections, and support programs for smaller businesses to minimize financial burdens. Broad public support, coupled with evidence of consumer harm from dark patterns, would also be essential to counter lobbying efforts and gain political momentum for passing such legislation.

- Technological Barriers

1. Complexity of Detection Algorithms: Dark patterns vary widely across platforms, making them difficult to identify using one-size-fits-all algorithms. Many manipulative tactics are context-specific, requiring highly adaptable machine learning models. Building and maintaining a real-time detection system for such a broad range of patterns across digital interfaces is both complex and resource-intensive.

2. Integration with Legacy Systems: Many companies, especially larger ones, rely on older systems for their digital interfaces. Integrating new detection technology with these legacy systems could be challenging and costly, creating a potential technical and operational barrier.

3. Adaptability and Evolving Dark Patterns: Dark patterns constantly evolve to circumvent detection, necessitating continuous updates to detection models. Developing a solution that can automatically adapt to new and evolving dark patterns without manual updates is a complex problem that existing technology does not fully address.

- Financial Barriers

1. High Development and Maintenance Costs: The proposed solution involves significant upfront and ongoing costs for AI development, system maintenance, and compliance support. Small- and medium-sized enterprises (SMEs) may find these costs prohibitive, creating an entry barrier and raising concerns about competitive disadvantage.

2. Revenue Impact: Many companies benefit financially from dark patterns, especially in e-commerce, subscription-based services, and digital advertising. Removing these practices could lead to an initial decline in conversion rates and revenue, making companies hesitant to support or comply with the proposal.

3. Corporations and Industries Utilizing Dark Patterns: E-commerce and Subscription-Based Services: Many companies in these sectors rely on dark patterns to drive

conversions, increase average transaction value, and retain customers. They may resist regulations that would reduce their ability to leverage these tactics, as it could impact their revenue and customer acquisition strategies.

4. Online Advertising and Marketing Agencies: Advertising agencies and digital marketers often employ tactics like misdirection and confirm-shaming to influence consumer behavior. New restrictions on dark patterns may limit their strategies, which could lead to industry pushback.

5. Major Platforms (e.g., Amazon, Google, Facebook): These platforms may use subtle manipulative tactics to enhance user engagement or data collection, so limitations on dark patterns could disrupt their business models. Given their extensive resources, these companies are likely to lobby against regulations that could impose compliance costs and impact their growth.

6. App Developers and Mobile Platforms: In-app purchases and retention mechanisms often rely on dark patterns to encourage users to continue engaging or purchasing within apps. Developers may resist restrictions that could reduce their revenue, particularly for free apps that depend on in-app monetization.

- Regulatory and Compliance Barriers

1. International Compliance: Dark patterns are a global issue, yet the legal environment varies widely across jurisdictions. Implementing a consistent framework would require international regulatory alignment, which can be difficult given differing consumer protection laws, privacy regulations, and enforcement mechanisms.

2. Lack of Precedent and Standards: Regulatory agencies currently lack established standards for dark pattern detection and classification, which makes drafting a universally acceptable regulatory framework challenging. Defining, categorizing, and setting detection thresholds for dark patterns across sectors will require significant research and consensus-building.

- User Privacy Concerns

1. Data Collection and User Privacy: For the system to detect dark patterns in real time, it would need to analyze user interactions, which could raise concerns about data privacy and surveillance. Ensuring that the system complies with data protection regulations like GDPR and CCPA without infringing on user privacy is a challenging balance to strike.

6.2.5 Cost Estimation for the Proposed Solution

Data Collection and Preparation

1. **Synthetic Data Generation**

   Costs here depend on the complexity and volume of synthetic data generated. Using generative models or simulation tools could entail costs for specialized software and computational resources.

2. **Annotated Real-world Data**

   If leveraging real-world data with annotated dark patterns, the associated costs would cover either data purchase (if commercially available) or a team for manual annotation.

Model Fine-tuning

1. **Computational Resources**

   Given that fine-tuning CLIP is computationally intensive, expect significant expenses if using cloud-based GPUs/TPUs, with costs scaling based on the number of training epochs and model updates.

2. **Infrastructure**

   If conducted on-premise, hardware acquisition (such as high-performance GPUs or TPUs) will incur substantial upfront costs. Maintenance, power, and cooling are also factors.

Model Deployment and Maintenance

1. **Deployment Infrastructure**

   Hosting and integrating the fine-tuned model into a production system could require additional costs, particularly for storage and cloud deployment on scalable servers.

2. **Regular Updates**

   As dark patterns change, periodic model retraining will be necessary, leading to recurring computational and data generation costs.

7 Software Requirement Specification

1. Project Initialization and Requirements Gathering

Stakeholder Collaboration

- Work with regulatory bodies (e.g., FTC, European DPAs) and industry representatives to finalize requirements, identify target dark patterns, and define data privacy and security standards.

Requirement Documentation

- Define system requirements, including real-time pattern detection, anonymized reporting, compliance alerts, and adaptive learning capabilities.

Technology Selection

- Choose frameworks for AI model development (e.g., TensorFlow, PyTorch), browser extension and app development (e.g., Chrome Extensions API, iOS/Android SDKs), and cloud infrastructure for data processing (e.g., AWS, Google Cloud).

2. Development Phases by Layer

Layer 1: User Interface (UI) Layer Development

Browser Extension and Mobile App Integration

- Develop a lightweight browser extension using the Chrome or Firefox Extensions API to intercept and analyze UI elements.
- Build app integrations for Android and iOS using SDKs to detect dark patterns in mobile applications.
- Implement a notification module to alert users when dark patterns are detected, giving users an option to report the instance.

User Interaction and Reporting Module

- Build a simple, intuitive interface that allows users to report dark patterns by clicking on specific flagged elements.
- Integrate a consent prompt for users to allow anonymous data reporting, complying with privacy regulations.

Layer 2: Detection Layer (AI-Powered) Development

Data Collection and Training Set Creation

- Collect and curate a dataset of UI patterns labeled as misdirection, confirmshaming, framing, etc. This can include both open-source datasets and synthetic data from mock websites.
- Annotate the data with pattern types, utilizing human input and crowd-sourced labels to ensure accuracy and reduce bias.

Dark Pattern Detection Model

- Train a convolutional neural network (CNN) or/and Natural Language Processing (NLP) model to detect dark pattern elements in UI design, such as misleading button placement or guilt-inducing text.
- Build a Pattern Classification Module within the model, using supervised learning to classify detected dark patterns by type.
- Regularly retrain and validate the model using feedback from real user reports and updates to pattern libraries.

Adaptive Learning System

- Implement an adaptive learning feature that continuously learns from flagged patterns, updating its training set with newly detected patterns and human-reviewed reports.
- Use reinforcement learning to improve detection accuracy, focusing on reducing false positives and negatives.

Layer 3: Reporting and Analytics Layer Development

Automated Reporting Pipeline

- Develop a data anonymization pipeline that strips personally identifiable information (PII) from flagged pattern data, ensuring GDPR, CCPA, and similar compliance.
- Set up a cloud-based data storage and processing system (e.g., AWS Lambda with DynamoDB or Google BigQuery) to store and process reports at scale.

Regulatory Analytics Dashboard

- Create a dashboard using a framework like Power BI or Tableau, allowing regulatory bodies to monitor trends, flag reports, and visualize dark pattern usage across industries.
- Implement analytics features to display data points, such as frequently reported companies, common dark pattern types, and geographic distribution of reports.

Layer 4: Policy Compliance and Notification Layer Development

Compliance Monitoring and Alerting Module

- Set up an automated compliance engine that cross-references reported patterns against legal standards (GDPR, DSA, CCPA, etc.).
- Implement rule-based alerts to notify companies when dark patterns are detected on their websites or apps. These alerts can specify the type of pattern, the corresponding regulation, and potential penalties for non-compliance.

Integration with Regulatory APIs

- If available, integrate with APIs from regulatory bodies to streamline reporting and compliance notifications. This could include report submission APIs for filing with organizations like the FTC or EU authorities.

Penalty Management System

- Develop a penalty tracking system to manage warnings and fines for repeat offenders. This can be a simple database that tracks companies, offenses, and actions taken.

3. Testing and Validation

- **Initial Testing:** Test each component independently with synthetic data to ensure accuracy, privacy, and usability. Check for false positives and negatives in the detection model to refine the algorithm.
- **User Testing:** Conduct user trials with consented participants to verify that the system flags patterns accurately and that the reporting process is user-friendly.
- **Regulatory Testing:** Collaborate with regulatory agencies to validate that flagged patterns match legal definitions and that data collection meets compliance standards.

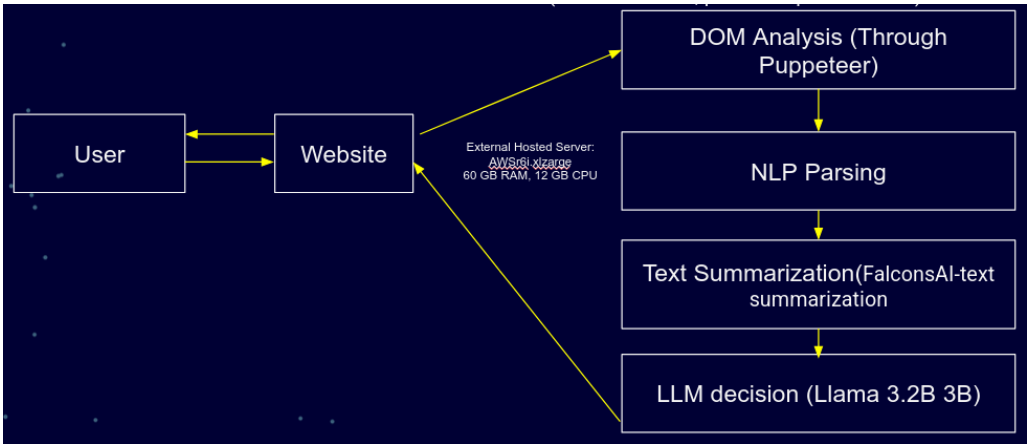
4. Deployment and Integration

- **Staged Rollout:** Begin with a pilot program on major web browsers and popular apps to gather initial data and refine detection algorithms.
- **Real-Time Monitoring and Feedback Loop:** Continuously monitor system performance, adjusting detection algorithms based on user feedback and updates to dark pattern definitions.
- **Scaling and Expansion:** After successful pilot testing, scale the system for broader deployment across browsers, platforms, and regions.

5. Maintenance and Continuous Improvement

- **Ongoing Model Training:** Regularly update the AI model with new patterns and conduct regular accuracy tests, leveraging feedback from users and regulatory changes.
- **Privacy and Compliance Audits:** Conduct frequent audits to ensure data handling, storage, and processing meet evolving privacy and data protection standards.
- **User and Regulatory Feedback Integration:** Integrate user feedback and regulatory updates into the system, adapting detection mechanisms for newly defined dark patterns.

Figure 2: Proof-of-Concept: Detection Layer Architecture



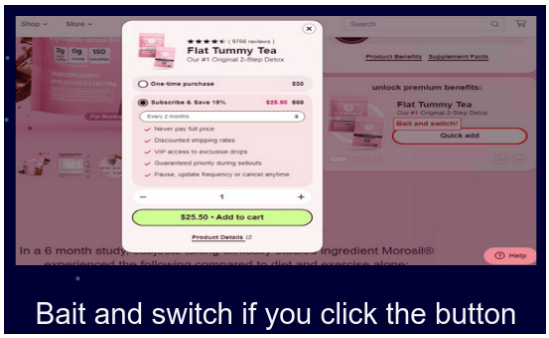


Figure 3: Dark pattern: Bait and switch

Figure 4: Dark pattern notified to user

Figure 5: Bait and Switch Detection

8 Proof-of-Concept - Layer 2: Detection Layer

The Dark Pattern Detection LLM system combines DOM analysis and LLM-based summarization to identify bait-and-switch patterns on websites. The system performs DOM analysis to extract and analyze webpage elements, returning bounding boxes to highlight specific regions, such as misleading links. It uses Llama 3.2B to summarize the content of a webpage, compare it to the content of the previous page, and generate a similarity score to identify discrepancies. For nuanced detection, the LLM evaluates contextual information and generates detailed responses, which are further processed into simple binary outcomes (e.g., "Yes" or "No"). This integrated approach enables precise detection and visualization of manipulative design elements. 2 shows the architecture diagram of the prototype implementation. 5 shows the screenshots captured how the system detects the dark pattern in the background while the user interacts with the website.

References

[1] Amos Tversky and Daniel Kahneman. The framing of decisions and the psychology of choice. *Science*, 211(4481):453–458, 1981.

[2] Amos Tversky and Daniel Kahneman. Judgment under uncertainty: Heuristics and biases. *Science*, 185(4157):1124–1131, 1974.

[3] Kim Huat Goh and Jesse C. Bockstedt. The Framing Effects of Multipart Pricing on Consumer Purchasing Behavior of Customized Information Good Bundles. *Information Systems Research*, 24(2):334–351, June 2013.

[4] Idris Adjerid, Alessandro Acquisti, and George Loewenstein. Choice architecture, framing, and cascaded privacy choices. page mnsc.2018.3028.

[5] Gediminas Adomavicius, Jesse Bockstedt, Shawn Curley, and Jingjing Zhang. Do recommender systems manipulate consumer preferences? a study of anchoring effects. *SSRN Electronic Journal*, 24, 12 2013.

[6] Harry Brignull, Gerry Duffy, Colin Eagan, Jeffrey MacIntyre, Ste Grainer, Aaron Gustafson, and Jeffrey Zeldman. Dark patterns: Deception vs. honesty in ui design, Nov 2011.

[7] Marshini Chetty Arvind Narayanan, Arunesh Mathur and Mihir Kshirsagar. Dark patterns: Past, present, and future the evolution of tricky user interfaces.

[8] Kimberly Adams and Sarah Leeson. Frustrating user-experience tactics can have real harm, "dark pattern" expert says, Aug 2022.

[9] George Loewenstein, Cass R. Sunstein, and Russell Golman. Disclosure: Psychology changes everything. *Annual Review of Economics*, 6(Volume 6, 2014):391–419, 2014.

[10] Andreas T. Schmidt and Bart Engelen. The ethics of nudging: An overview. *Philosophy Compass*, 15(4):e12658, 2020.

[11] Neil Levy. Autonomy and addiction. 36(3):427–447.

[12] Arunesh Mathur, Gunes Acar, Michael J. Friedman, Eli Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan. Dark patterns at scale: Findings from a crawl of 11k shopping websites. *Proc. ACM Hum.-Comput. Interact.*, 3(CSCW), November 2019.

[13] Colin M. Gray, Jingle Chen, Shruthi Sai Chivukula, and Liyang Qu. End user accounts of dark patterns as felt manipulation. 5:1–25.

[14] N. Eyal and R. Hoover. *Hooked: How to Build Habit-Forming Products*. Penguin Publishing Group, 2014.

[15] Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L. Toombs. The dark (patterns) side of UX design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–14. ACM.

[16] Tony Tobin Danny Gilbert. Dark patterns explained.

[17] Jamie Luguri and Lior Jacob Strahilevitz. Shining a Light on Dark Patterns. *Journal of Legal Analysis*, 13(1):43–109, 03 2021.

[18] Dark patterns: Past, present, and future.

[19] Kim Huat Goh and Jesse C. Bockstedt. The framing effects of multipart pricing on consumer purchasing behavior of customized information good bundles. 24(2):334–351.

[20] Justin Elliott. Turbotax just tricked you into paying to file your taxes, April 22 2019. Accessed: 2024-10-01.

[21] Federal Trade Commission. Ftc sues owner of online dating service match.com for using fake love ads, September 25 2019. Accessed: 2024-10-01.

[22] GDPR Info. General data protection regulation (gdpr), 2024. Accessed: 2024-10-01.

[23] California Privacy Protection Agency. California privacy protection agency (cppa), 2024. Accessed: 2024-10-01.

[24] Artificial Intelligence Act. The artificial intelligence act, 2024. Accessed: 2024-10-01.

[25] Ari Ezra Waldman. Cognitive biases, dark patterns, and the 'privacy paradox'. 31:105–109.

[26] Van Tran, Aarushi Mehrotra, Ranya Sharma, Marshini Chetty, Nick Feamster, Jens Frankenreiter, and Lior Strahilevitz. Dark patterns in the opt-out process and compliance with the california consumer privacy act (CCPA).

[27] Shaowen Bardzell, Jeffrey Bardzell, Jodi Forlizzi, John Zimmerman, and John Antanitis. Critical design and critical theory: the challenge of designing for provocation.

[28] Jeffrey Bardzell, Shaowen Bardzell, and Erik Stolterman. Reading critical designs: supporting reasoned interpretations of critical design. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1951–1960. ACM.

[29] Batya Friedman, Peter H Kahn, and Alan Borning. Value sensitive design: Theory and methods.

[30] Daniel Berdichevsky and Erik Neuenschwander. Toward an ethics of persuasive technology. 42(5):51–58.

[31] Arunesh Mathur, Jonathan Mayer, and Mihir Kshirsagar. What makes a dark pattern... dark? design attributes, normative considerations, and measurement methods. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–18.

[32] Abby L. Stemler. Antitrust, data, and privacy: An impossible tug of war for internet companies. *Alabama Law Review*, 72(1):1–45, 2020. Accessed: 2024-10-01.

[33] Weiwei Yi and Zihao Li. Mapping the scholarship of dark pattern regulation.

[34] Greenwoods & Herbert Smith Freehills. Dark patterns explained, 2024. Accessed: 2024-10-01.

[35] Berkeley Technology Law Journal. Exposing dark patterns: Are they harboring anticompetitive practices?, April 2024. Accessed: 2024-10-01.

[36] Philip Di Salvo. Leaking black boxes: Whistleblowing and big tech invisibility.

[37] Consumer Watchdog. Dark patterns are steering many internet users into making bad decisions, 2024. Accessed: 2024-10-01.

[38] Lin Kyi, Sushil Ammanaghatta Shivakumar, Cristiana Teixeira Santos, Franziska Roesner, Frederike Zufall, and Asia J. Biega. Investigating deceptive design in gdpr's legitimate interest. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI '23, New York, NY, USA, 2023. Association for Computing Machinery.

[39] Gabriela Zanfir-Fortuna. Follow the (personal) data: Positioning data protection law as the cornerstone of eu's 'fit for the digital age' legislative package. *SSRN Electronic Journal*, 01 2024.

[40] Carol Moser, Sarita Y. Schoenebeck, and Paul Resnick. Impulse buying: Design practices and consumer needs. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–15. ACM.

[41] Federal Trade Commission. Federal trade commission announces final "click-to-cancel" rule, making it easier for consumers to end recurring subscriptions, 2024. [Accessed: 2024-10-27].

[42] California Attorney General's Office. California consumer privacy act (ccpa), 2024. [Accessed: 2024-10-27].

[43] California Privacy Protection Agency. Consumer privacy act regulations, 2024. [Accessed: 2024-10-27].

[44] U.S. Senate. Detour act, s.3330, 117th congress, 2022. Accessed: 2024-10-28.

[45] California Legislature. Assembly bill no. 2863, 2023-2024 session, 2024. [Accessed: 2024-10-27].

[46] Office of Senator John Thune. Schatz, thune, warnock, kennedy introduce new legislation to stop deceptive subscription business practices, 2021. [Accessed: 2024-10-27].

[47] Federal Trade Commission. Federal trade commission - policy, 2024. [Accessed: 2024-10-27].

[48] Federal Trade Commission. Can-spam act compliance guide for business, 2024. [Accessed: 2024-10-27].

[49] U.S. Congress. 15 u.s. code § 13 - discrimination in price, services, or facilities (robinson-patman act), 2024. [Accessed: 2024-10-27].