

Regulating Deceptive Design: A Comparative Analysis of U.S. and EU Laws on Dark Patterns

Justin Eric Chen
University of Illinois Urbana-Champaign
jechen4@illinois.edu

Ece Gumusel
University of Illinois Urbana-Champaign
eceg@illinois.edu

Joshua Sutton
Grinnell College
suttonjo@grinnell.edu

Kyrie Zhixuan Zhou
University of Texas at San Antonio
kyrie.zhou@utsa.edu

Sang-Hwa Oh
University of Illinois Urbana-Champaign
sanghwa2@illinois.edu

Abstract

With the expansion of digital interactions, users are increasingly subject to dark patterns—interface designs intended to manipulate decision-making. Regulatory responses from the European Union (EU) and the United States (US) aim to mitigate these practices, yet protections remain inconsistent across jurisdictions. Despite growing concern, there is limited research comparing how EU and US regulations approach dark patterns. This paper conducts a thematic analysis and word frequency test of relevant regulations, finding that EU frameworks insufficiently address specific technological risks and lack extended safeguards for vulnerable groups. In contrast, US regulations fall short in governing gatekeepers' use of manipulative designs and lack robust oversight of artificial intelligence (AI) systems. The paper concludes with recommendations, including expanding protections for vulnerable users in the EU and strengthening gatekeeper and AI-related provisions in the US.

Keywords: Dark Patterns, Ethics, Policy, Artificial Intelligence (AI), HCI, Governance

1. Introduction

Dark patterns or also know as deceptive patterns can be described as “a user interface that has been carefully crafted to trick users into doing things, such as buying insurance with their purchase or signing up for recurring bills” (Brignull, 2023, p. 5). The main purpose of deceptive patterns is to impede the consumers' ability to make informed choices (Gray et al., 2018a). As deceptive patterns drew attention, the EU's General Data Protection Regulation (GDPR) required consent to be freely given, specific, informed, and unambiguous,

effectively prohibiting manipulative design (European Parliament and Council of the European Union, 2016). The GDPR established a foundational framework that shaped later policies and set a global precedent for regulating deceptive design. Its impact extends globally, influencing privacy laws in regions such as the United States. For example, the California Consumer Privacy Act (CCPA), enacted in 2018 and effective in 2020, was the first comprehensive state privacy law in the US, shaped by the GDPR and rising concerns over digital harms (Mulgund et al., 2021).

Despite efforts against deceptive patterns, EU regulations lack a unified definition, hindering consistent enforcement across member states (Car & Cassetti, 2025). Scholars note that this ambiguity lets platforms continue manipulative design, highlighting the need for a unified EU definition (Car & Cassetti, 2025; Herman, 2024; Santos et al., 2024). US laws tend to be reactive, addressing issues only after harm occurs (Solove, 2021). Most also research examines US privacy laws in isolation, without considering their place in the broader regulatory patchwork (King & Stephan, 2021; Tran et al., 2025). Many scholars focus on CCPA because it is a landmark regulation that affects over 40 million Californians and approximately 500,000 businesses, including 10% of Fortune 1000 companies (Helveston, 2018)

This fragmented approach overlooks the complex interactions and potential overlaps between different laws and regulations, which can significantly affect their overall effectiveness in addressing deceptive patterns. Furthermore, little work has been done to systematically compare the US and EU regulatory frameworks as a whole. A comparative analysis is essential to reveal each system's strengths and weaknesses and to explore how one jurisdiction can inform improvements in the

other. Accordingly, this study focuses on US and EU law, reflecting their global influence and the scholarly urgency to understand how they address deceptive patterns (Car & Cassetti, 2025; Gunawan et al., 2021; Herman, 2024; King & Stephan, 2021; Santos et al., 2024). Although countries like Canada and Australia have regulations on deceptive patterns, literature on these is limited. The US and EU are selected for their scholarly coverage, regulatory approaches, and global influence, making them most informative for comparative analysis at this stage. To guide this analysis, the study poses the following research questions:

1. What are the key similarities and differences between EU and US regulatory approaches to deceptive patterns?
2. What gaps exist in the regulation of deceptive patterns in both the European Union and the United States?

2. Related Work

Current work in Information Systems (IS) has begun to address the topic of deceptive patterns, but most of the literature on deceptive patterns are on the effects of deceptive patterns on user's well being, autonomy, and trust (Kollmer & Eckhardt, 2023; Singh et al., 2025; Witte et al., 2023). Little work has been done on regulatory practices within the field of IS. This related work section introduces the existing research on US and EU regulations.

2.1. EU Regulations on Deceptive patterns

Considerable research examines how EU regulations address deceptive patterns. Scholars agree that the EU actively pushes regulations, but many lack a unified legal definition (Car & Cassetti, 2025; Herman, 2024; Santos et al., 2024). For example, the Digital Service Act emphasizes distortion and impairment, while the Data Act emphasizes deception, highlighting the challenges of harmonizing compliance standards (European Parliament and Council, 2022, 2023). This disconnection makes it difficult to determine which law applies when multiple frameworks govern the same issue, potentially leading to under- or over-enforcement due to regulatory fragmentation (Graef, 2023). The inconsistent definitions makes regulating deceptive patterns even harder because deceptive patterns already exist in the gray area as deceptive patterns act in both legitimate persuasive techniques and illegal methods of coercion and manipulation (Brenncke, 2024). Because

of this inconsistency, scholars like Lesier and Santos (2023) argue that there should be a clear labeling of deceptive patterns for enforcement.

2.2. US Regulation on Deceptive Patterns

US studies on deceptive patterns focus primarily on the CCPA and its amendment, the California Privacy Rights Act (CPRA). King and Stephan (2021) examine challenges in defining and regulating privacy-focused deceptive patterns, review existing approaches, discuss measurement difficulties, and offer policy recommendations. Similarly, Gunawan et al. (2021) explore the shortcomings of both the DETOUR Act and the CPRA, and propose a more robust definition of deceptive patterns. For example, the DETOUR Act does not define deceptive patterns but outlines practices companies may or may not engage in online (U.S. Congress, 2023). The CCPA also does not provide a definition, stating that: "Dark pattern means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice, as further defined by regulation" (California Legislature, 2018). The CCPA's definition of deceptive patterns remains vague, with "as further defined by regulation" deferring details to future rulemaking and creating legal uncertainty.

Few studies examine other standards, such as the Federal Trade Commission (FTC), which scholars argue provides inadequate and inefficient guidance on deceptive patterns (Lalsinghani, 2024; Wilson, 2023). Lalsinghani 2024 argue how FTC has faced difficulties in deciding how far its regulatory power should extend. Wilson 2023 talks about how the regulations can only hold them accountable through consent decrees and nonmonetary penalties, rather than imposing fines or stronger punishments.

3. Methodology

3.1. Law Document Selection

The study conducts a review of data protection and privacy laws and regulations in both the EU and the US to understand regulatory approaches regarding deceptive patterns. This study selected laws and regulations that (1) explicitly mention or functionally regulate deceptive patterns or deceptive interface design; (2) are binding laws rather than guidelines, holding platforms accountable for deceptive design practices; and (3) are relevant to privacy, consent, or consumer choice.

Based on these criteria, the study selected the following documents from the EU: the Digital Services Act (DSA), Digital Markets Act (DMA), Unfair

Commercial Practices Directive (UCPD), Data Act, AI ACT and GDPR which collectively address platform governance, data protection, and manipulative practices (Car & Cassetti, 2025; Herman, 2024).

For US regulations, the study selected the CCPA and its amendment, the California Privacy Rights Act (CPRA), the Connecticut Data Privacy Act (CDPA), the FTC Act – Section 5, and Deceptive Experiences To Online Users Reduction Act (DETOUR Act) all of which include provisions addressing manipulative consent flows (Gunawan et al., 2021; Lalsinghani, 2024; Mathur et al., 2021; Nousiainen & Perdomo Ortega, 2023).

3.2. Data Analysis

To analyze the regulatory landscape of deceptive patterns, we use a thematic analysis based on Braun and Clarke’s framework to guide coders in identifying emerging themes (Braun & Clarke, 2006). The emerging themes and sub-themes were organized into a hierarchical structure using XMind, a mind-mapping tool to organize the themes, sub-themes, and supporting quotations for synthesis and presentation. In doing so, thematic analysis allows us to systematically identify and interpret patterns across complex regulatory texts, providing a structured and rigorous approach to synthesize the data.

The study used NVivo word frequency analysis to identify sections with potentially relevant terms. The word frequency test provides a systematic way to detect recurring words across multiple lengthy documents. This ensures that frequently mentioned regulatory terms are captured and guiding subsequent in-depth thematic coding. The results of the word frequency analysis were used to help guide the initial development of thematic coding and the results of the word selection from the frequency analysis are reported in the Results section (see Table 1).

The lead coder reviewed the frequency list to flag potentially manipulative terms, which were then discussed with the other coders until consensus was reached. These keywords guided analysis of the surrounding context to determine whether they reflected manipulative design, forming the basis of the study’s findings.

Following the word frequency analysis, three coders conducted a thematic analysis on the ten selected legal documents. Each coder then independently reviewed the full texts of the assigned documents: Coder 1 reviewed four documents, while Coders 2 and coder 3 each reviewed three. Each coder applied open coding to identify recurring concepts and themes

related to manipulative or deceptive design. The lead coder synthesized the independent code sets into a consolidated framework, which the other coders reviewed to resolve disagreements and reach consensus on the final codes and themes.

4. Results

The results section presents key themes identified through team consensus during thematic analysis, including Defending Against Deceptive Patterns, Security, Transparency, User Autonomy, and Regulation. In addition, a word frequency test supported the document analysis, with the most frequent terms shown in Table 1.

4.1. Regulations

The coding of the eleven documents revealed three sub-themes: definitions, regulatory enforcement, and risk assessment. These sub-themes illustrate how different jurisdictions structure, implement, and evaluate their regulatory frameworks.

4.1.1. Definition Both U.S. and EU regulations define manipulative practices to protect users, including issues like personal data, dark patterns, consent, and profiling. There are subtle differences between these regulations; for example, the U.S. defines dark patterns based on how they impair self-determination and autonomous decision-making. As stated in the CDPA,

“Dark pattern” means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice”

In contrast, the EU defines dark patterns more in terms of their deceptive nature and the negative consequences they produce for consumers, particularly by nudging them into unwanted behavior or impairing their free choice. An example can be seen in the Data Act,

“Dark patterns are design techniques that push or deceive consumers into decisions that have negative consequences for them.”

4.1.2. Regulation Enforcement Both US and EU regulations enforce rules to prevent manipulative design on digital platforms. The similarity lies in that both regulations have penalties for violations. For example, the US regulation CCPA states,

Document	Key Terms/Themes
AI Act (EU)	control, prohibitions, security, transparency, manipulative, bias, vulnerable, influence, consent, users
Data Act (EU)	user, access, rights, requires, unfair, undue, control, choice, transparent, undermine, privacy, abuse, influence, consent, deceive, manipulating, dark
Digital Markets Act (EU)	gatekeeper, unfair, power, choice, default, misleading, interfaces
Digital Services Act (EU)	design, interface, presented, language, clear, undue, transparency, user, choice, targeting, control, profiling, manipulative, misleading, influence, meaningful
GDPR (EU)	information, obligations, consent, compliance, complaint, security, prejudice, free, profiling, transparent, clear, automated, undue, fair, default, meaningful
UCDP (EU)	informed, misleading, aggressive, false, omission, choice, presentation, undue, coercion, harassment, inertia, control, confusion, deceive, exploitation, consent, vulnerable, ambiguous
DETOUR Act (US)	user, online, consent, behavioral, psychological, informed, deceptive, review, standards, design, autonomy, compulsive, enforcement, interface, manipulate, privacy, subverting, exploitative, clear, disclosure, obscured, affirmative, representation, transparent
CDPA (US)	data, controller, consumer, personal, processing, information, opt, advertising, privacy, consent, disclosure, clear, pattern, dark, unfair, deceptive, autonomy, behavior, interface
CCPA (US)	informed, consumer, personal, agency, privacy, opt, protection, disclosure, consent, advertising, behavioral, choices, clearly, deceptive, user, affirmatively, avoid, represent
FTC (US)	unfair, deceptive, conditions, representation, advertising, misleading, clearly, ensure, disclosures, claims, review, avoid, promotional, omission, conditions, informed, claims, affirmatively, misled, misrepresent

Table 1. Words Selected from the Word Frequency Test

“Any business, service provider, contractor, or other person that violates this title shall be liable for an administrative fine of not more than ...(\$2,500) for each violation ... or ...(\$7,500) for each intentional violation ...”

As for the EU regulations, the Digital Market Act states:

“The Commission may adopt a decision, imposing on undertakings... fines not exceeding 1% of their total worldwide turnover ... year where they intentionally or negligently”

The difference in these penalties lies in how they are calculated. For example, under the Digital Markets Act, fines can reach up to 1% of a company’s global annual turnover for certain violations, making the penalty scale with the size of the business. In contrast, US laws like the CCPA impose flat-rate fines — typically \$2,500 to \$7,500 per violation — which are not tied to a company’s revenue.

4.1.3. Risk Assessment The US and EU both use legal frameworks to protect individuals from deceptive

practices, but their approaches differ in scope and values. Both the US and the EU are similar in that they both require the performance of a risk assessment to evaluate whether a practice or technology poses a danger to users. For example, the US FTC Act states,

“A three-part test is used to determine whether a representation, omission, or practice is “deceptive.””

As for the EU regulations, the Digital Services Act states,

“Providers of very large online platforms and search engines shall diligently identify, analyse and assess any systemic risks ... stemming from the design or functioning of their service ... or from the use made of their services”.

The difference lies in the fact that US regulations, particularly under the FTC Act, incorporate risk assessments focused on manipulative design by encouraging an analysis of why a deceptive act may be considered unfair. The FTC states:

Public policy may also be considered in

the analysis of whether a particular act or practice is unfair.

The EU regulations, on the other hand, focus on systemic risk assessments related to services and technologies, including algorithmic risks and fundamental rights impacts, but do not frame it in terms of "unfairness" like the FTC does. For example, the Digital Services Act requires search engines and large online platforms to identify and assess systemic risks related to their services, including risks from algorithmic systems.

4.2. Defending Against Deceptive patterns

The second common main theme identified from analyzing the documents revealed two main sub-themes: Combating/Prohibiting Dark Patterns and Protection of Vulnerable Groups. Below, we explore each of these sub-themes in detail.

4.2.1. Combating/Prohibition Dark Patterns The US and EU regulations exhibit similarities in their approach to prohibiting misleading or manipulative conduct. For example, the GDPR, an EU regulation, states:

"It shall also be regarded as a misleading omission when ... a trader hides or provides ... material information ... or fails to identify the commercial intent ... and ... this causes or is likely to cause the average consumer to take a transactional decision that he would not have taken otherwise".

The DETOUR Act, a US regulation, states,

"It shall be unlawful for any large online operator— (1) to design, modify, or manipulate a user interface with the purpose or substantial effect of obscuring, subverting, or impairing user autonomy... to obtain consent or user data".

From these two examples, it is clear that both regulations address not only manipulative practices themselves but also their effects on users. Despite sharing the common goal of protecting users from such manipulative actions, there are subtle differences between them. As seen in the quoted section of the DETOUR Act, the focus is more directly on prohibiting manipulative user interface design practices.

In contrast, EU regulations, such as the GDPR, place greater emphasis on the clarity and transparency of

communication—an approach that can also influence UI design.

4.2.2. Protection of Vulnerable Group When it comes to the protection of vulnerable groups, EU regulations place a strong emphasis on safeguarding children, while US regulations take a broader approach that includes other vulnerable populations. For example, the Digital Markets Act (EU) states:

"Children merit specific protection with regard to their personal data in particular as regards the use of their personal data for the purposes of commercial communication or creating user profiles".

The US, however, focuses on a broader range of vulnerable groups, including the elderly and the financially vulnerable. Regulations such as the FTC extend protections beyond children to include these populations. As stated:

"Determine whether the bank tailors advertisements, promotional materials, and marketing scripts ... to the sophistication and experience of the target audience, including the elderly and financially vulnerable."

4.3. Security

The third main theme identified from analyzing the documents is security. This theme is further divided into two sub-themes: Cybersecurity Measures and User Data Privacy. The following sections explore the similarities and differences between US and EU policies in these areas.

4.3.1. Cybersecurity Measurements Both the US and EU regulations have taken security measures to protect the user's information and data. For example, Digital Markets Act and AI Act emphasize protecting users and infrastructure through justified and proportionate security measures. The same applies to US regulations as CCPA requires businesses to implement reasonable security procedures to protect personal information. However, what lies the difference is where EU regulations pays more attention in making sure important systems such as AI and software applications are secure and work correctly. For example, the Digital Market Act states,

"... it should be possible for the gatekeeper to implement strictly necessary and

proportionate measures if the gatekeeper demonstrates that such measures are justified and that there are no less-restrictive means to achieve that goal.”

On the other hand, US regulations place greater emphasis on consumer data privacy and business responsibilities. An example of the emphasis on consumer data privacy is found in the CPRA, which states:

“A business that collects a consumer’s personal information shall implement reasonable security procedures and practices...to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure...”

Although US regulations emphasize protecting consumer data privacy and holding businesses accountable for data protection, they lack specific measures addressing AI security. In contrast, the EU has enacted dedicated legislation for this purpose, known as the AI Act. The AI Act includes measures that address technical vulnerabilities specific to AI systems, such as model poisoning and adversarial inputs. The AI Act states,

“The technical solutions to address AI specific vulnerabilities shall include ... measures to prevent, detect, respond, resolve and control for attacks trying to manipulate the training data set ... inputs designed to cause the AI model to make a mistake ... confidentiality attacks or model flaws.”

4.3.2. User Data Privacy Both the US CPPA and the EU GDPR emphasize protecting user data privacy, specifically by safeguarding sensitive or confidential information. For example, the US regulation CPPA states,

“Any controller in possession of de-identified data shall: (1) take reasonable measures to ensure that the data cannot be associated with an individual; (2) publicly commit to maintaining and using de-identified data without attempting to reidentify the data; and (3) contractually obligate any recipients...”

As for the EU regulations, the GDPR states,

“The confidential information which the Union and national statistical authorities collect for the production of official European and official national statistics should be protected.”

The differences between these regulations are that CCPA focuses more on consumers’ control of personal data collection and use, and the EU places more emphasis on fundamental rights, such as privacy, freedom of assembly, and protection from surveillance. For example, the AI Act states,

“The use of AI systems for ‘real-time’ remote biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement is particularly intrusive to the rights and freedoms of the concerned persons, to the extent that it may affect the private life of a large part of the population, evoke a feeling of constant surveillance...”

On the other hand, the CCPA states,

“A business shall not collect additional categories of sensitive personal information or use sensitive personal information collected for additional purposes that are incompatible with the disclosed purpose ... without providing the consumer with notice consistent with this section”.

4.4. Transparency

Both the European Union and the United States incorporate transparency as a key element in their regulatory frameworks, though they approach it with different emphases and legal contexts. In the following subsection, we explore these regulatory approaches and the nuances that distinguish the US and EU frameworks.

4.4.1. Regulatory Approaches to Transparency in Data

US and EU regulations both emphasize the importance of clear transparency and user awareness concerning how personal data or AI-generated content is collected, used, and shared. For example, the US regulation CDPA states:

“A controller shall provide consumers with a reasonably accessible, clear and meaningful privacy notice”

The EU regulations, such as GDPR, state:

“The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes”.

The difference is that US laws often emphasize clear and truthful disclosure of product or service terms to protect consumers. For example, the FTC requires businesses to:

“Clearly disclose all material limitations or conditions on the terms or availability of products or services...”

In contrast, EU regulations embed transparency within a broader fundamental rights framework, extending beyond just consumer protection. The GDPR states:

“The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand...”

The EU also has specific protection over technologies that impact fundamental rights, emphasizing transparency in AI-generated content as the AI Act stated that:

“...it is appropriate to require providers of those systems to embed technical solutions that enable marking in a machine readable format and detection that the output has been generated or manipulated by an AI system and not a human”.

4.5. Human Autonomy

The fourth main theme that emerged from the analysis is human autonomy. This theme has been divided into three sub-themes: user consent, opt-in and opt-out rights, and default settings. These sub-themes reflect how regulations support individual control over digital interactions and data use.

4.5.1. User Consent Both EU and US regulations place significant emphasis on user consent, with many provisions requiring that consent be given through an affirmative, informed, and unambiguous act. For example, the CCPA states,

“...from using or disclosing the consumer’s sensitive personal information... unless the

consumer subsequently provides consent for... additional purposes.”

The EU regulations, such as GDPR, state,

“Consent should be given by a clear affirmative act ... such as by a written statement, including electronic means, or an oral statement.”.

There are some key differences in how consent is framed. The EU places consent within the context of fundamental rights, while the US takes a more consumer-oriented and contractual approach. For example, the CDPA emphasizes a “clear affirmative act signifying a consumer’s freely given, specific, informed and unambiguous agreement to allow the processing of personal data relating to the consumer.” In contrast, the EU treats consent as a rights-based safeguard. The EU treats consent as a rights-based safeguard. For example, the Digital Markets Act requires gatekeepers to comply with GDPR or anonymize data when consent is lacking, reinforcing individual rights protection.

4.5.2. Opt-In and Opt-Out Rights Both the US and the EU place strong emphasis on empowering users with the ability to opt in and out of personal data processing. In both jurisdictions, regulations require that users be provided with clear, conspicuous, and accessible information about data practices. For example, US regulations such as the CCPA states:

“Ensure that the opt-out preference signal is consumer-friendly, clearly described, and easy to use by an average consumer and does not require that the consumer provide additional information beyond what is necessary.”

Similarly, EU regulations such as the Digital Markets Act provide,

“The gatekeeper shall not degrade the conditions or quality of core platform services for users exercising their rights under Articles 5, 6, and 7...or make the exercise of those rights unduly difficult”.

US and EU regulations differ on gatekeeper restrictions. The EU explicitly prevents gatekeepers from degrading services or hindering data rights, showing stronger control over platforms. For example, the Digital Market Act states:

The gatekeeper shall not degrade the quality of core platform services for

users exercising their rights...or make the exercise of those rights unduly difficult...by subverting user autonomy or decision-making via the design or operation of a user interface.

On the other hand, the US focuses more on consumer choice and opt-out rights without specific language about gatekeepers' obligations not to degrade services or use design to frustrate choices. As CDPA provides,

"A consumer may designate an authorized agent...to exercise the rights of such consumer to opt out of the processing of such consumer's personal data."

GDPR requires active, affirmative consent and does not allow consent through silence, inactivity, or pre-ticked boxes. Active, affirmative consent is required. The US regulations CDPA also states that opt-out mechanisms must represent an affirmative, freely given, and unambiguous choice. Defaults cannot imply consent.

4.5.3. Default Setting The differences from these regulations lie in the way they view users' control over defaults. The EU approach requires active prompting of users to select alternatives, especially in core platform services. For example, the Digital Market Act states:

"This includes prompting a choice screen at the users' first use of an online search engine, virtual assistant, or web browser of the gatekeeper listed in the designation decision, allowing end users to select an alternative default service..."

On the other hand, the US approach is that the opt-out mechanism may be default, but must still represent an affirmative, unambiguous opt-out choice. As the CDPA provides:

"Not make use of a default setting, but, rather, require the consumer to make an affirmative, freely given and unambiguous choice to opt out of any processing..."

5. Discussion

Both US and EU regulations have largely approached deceptive design through privacy and security protections. Combating these deceptive techniques is important because they can lead to a loss of user privacy and undermine individual autonomy (Mathur et al., 2021). Thus, both regulations include safeguards to protect users from privacy-related issues.

However, framing deceptive design mainly as a privacy issue leaves significant gaps, since manipulative interfaces extend beyond data management. For example, the CDPA grants opt-out rights but does not restrict design tactics that frustrate or manipulate user choices. This gap is significant because protecting choice is not only about data preferences but also about safeguarding autonomy, privacy, and freedom from manipulation (Cate & Mayer-Schönberger, 2013). Without rights-based protections, deceptive designs undermine user control and trust. Even if those choices are clearly presented in text or buttons, the overall design of the interface can still manipulate the user's behavior (Gray et al., 2018b). This demonstrates that current regulations, which primarily focus on data and privacy, are insufficient to prevent manipulative interface designs from influencing user behavior.

These gaps are particularly concerning as technology evolves, introducing new manipulation techniques that current regulations do not adequately address. Beyond protecting fundamental rights, US regulations lack safeguards for AI. As AI is an emerging subject, new privacy risks are being put in the forefront. Some AI tools such as ChatGPT-based digital assistants that can read and write and are interactive with the web offer new opportunities for hackers (Clarke, 2023). Generative AI is known for enabling advanced persistent threats, as it can generate realistic content (pretexting) and analyze existing information (reconnaissance). This allows attackers to customize their malicious intent in the online space (Ansari et al., 2022).

EU regulations are not without faults either. While they excel at protecting individual rights, they are less focused on addressing consumer-specific harms. As online spaces become a more integral part of daily life, individuals may face deceptive marketing practices or financial exploitation in these environments (Sprague & Wells, 2010). This reflects a broader challenge in technology-neutral lawmaking. While broad policies covering all technologies offer general applicability, there remains a critical need for technology-specific regulations to address unique risks and, in this case, to effectively protect consumers' rights and prevent manipulation (Abiteboul & Stoyanovich, 2019; Hildebrandt & Tielemans, 2013; Shadikhodjaev, 2021). EU regulations also fail to protect vulnerable groups, like older or financially at-risk adults. This gap is especially concerning as the proportion of older adults is rapidly increasing compared to younger demographics due to declining fertility rates (Cotten et al., 2016; World Health Organization, 2021). Without explicit regulatory focus on these vulnerable groups, existing frameworks risk perpetuating inequalities and failing to safeguard

those most in need (Van Deursen & Helsper, 2015).

These findings reveal key gaps in current regulatory frameworks, especially in safeguarding user autonomy, preventing manipulative design, and protecting vulnerable populations. Regulations must go beyond general user rights and address deceptive interface designs. Thus, the US and EU should look to each other's regulatory approaches to improve their own frameworks. For example, the US should shift the burden of control on users. Instead, they should impose obligations on platforms to prevent manipulative design patterns that distort user autonomy. The US should also expand its regulations and address AI-specific manipulation risks. These should include transparency in AI decision-making, limitations on data usage, and safeguards against algorithmic manipulation. While the EU's focus on fundamental rights is essential, it should be complemented by stronger consumer protection measures addressing modern online risks.

Another area where EU regulation should be expanded is in the protection of older adults, low-income users, and others who are at disproportionate risk of harm, as current efforts primarily focus on children. Current US regulations lack adequate protections for children, but proposed legislation like the American Data Privacy and Protection Act (ADPPA) aims to address these gaps, though it has not yet been enacted as of 2025.

6. Conclusion

This study analyzed ten regulatory articles from the U.S. and EU using thematic analysis and word frequency tests. From this analysis, five key themes were identified: Defending Against Deceptive Patterns, Security, Transparency, User Autonomy, and Regulation. The study identified several shortcomings in both U.S. and EU regulations. The EU's focus on fundamental rights often neglects regulations targeting consumer harms and usability. In contrast, US regulations place the burden of managing digital risks on users. The study recommends that US regulations shift responsibility to platforms to curb manipulative design, while EU regulations adopt a less neutral approach to better protect vulnerable groups such as older adults, low-income individuals, and online consumers.

7. Limitations and Future Work

This study is limited by its focus on EU and US regulations, while other regions are also attempting to address this issue. Future work should examine the ADPPA once it is intact and other regions, such as

Asia or Africa, since regulatory approaches and digital environments vary and lessons may not generalize globally.

References

- Abiteboul, S., & Stoyanovich, J. (2019). Transparency, fairness, data protection, neutrality: Data management challenges in the face of new regulation. *Journal of Data and Information Quality (JDIQ)*, 11(3), 1–9.
- Ansari, M. F., Sharma, P. K., & Dash, B. (2022). Prevention of phishing attacks using ai-based cybersecurity awareness training. *Prevention*, 3(6), 61–72.
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2), 77–101.
- Brenncke, M. (2024). Regulating dark patterns. *Notre Dame J. Int'l Comp. L.*, 14, 39.
- Brignull, H. (2023). *Deceptive patterns: Exposing the tricks tech companies use to control you*.
- California Legislature. (2018). California consumer privacy act of 2018 [Accessed: 2025-05-23].
- Car, P., & Cassetti, F. (2025, January). Regulating dark patterns in the eu: Towards digital fairness [At a Glance, PE 767.191].
- Cate, F. H., & Mayer-Schönberger, V. (2013). Notice and consent in a world of big data. *International Data Privacy Law*, 3(2), 67–73.
- Clarke, L. (2023). Call for ai pause highlights potential dangers. *Science*, 380(6641), 120–121.
- Cotten, S. R., Yost, E. A., Berkowsky, R. W., Winstead, V., & Anderson, W. A. (2016). *Designing technology training for older adults in continuing care retirement communities*. CRC Press.
- European Parliament and Council. (2022). Regulation (eu) 2022/2065 on a single market for digital services [Official Journal L 277, 27 October 2022]. <https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng>
- European Parliament and Council. (2023). Regulation (eu) 2023/2854 on harmonised rules on fair access to and use of data [Official Journal L 2023/2854, 22 December 2023]. <https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng>
- European Parliament and Council of the European Union. (2016). General data protection regulation (gdpr): Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 [Official Journal of the European Union, L 119, 4 May 2016, pp. 1–88].

- Graef, I. (2023). The eu regulatory patchwork for dark patterns: An illustration of an inframarginal revolution in european law?
- Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018a). The dark (patterns) side of ux design. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–14. <https://doi.org/10.1145/3173574.3174108>
- Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018b). The dark (patterns) side of ux design. *Proceedings of the 2018 CHI conference on human factors in computing systems*, 1–14.
- Gunawan, J., Choffnes, D., Hartzog, W., & Wilsom, C. (2021). Towards an understanding of dark pattern privacy harms. *Position paper at the CHI 2021 Workshop: What can CHI do about dark patterns*.
- Helveston, M. N. (2018). Reining in commercial exploitation of consumer data. *Penn St. L. Rev.*, *123*, 667.
- Herman, J. (2024). Dark patterns: Eu’s regulatory efforts. *Security and Privacy*, *7*(6), e441.
- Hildebrandt, M., & Tielemans, L. (2013). Data protection by design and technology neutral law. *Computer Law & Security Review*, *29*(5), 509–521.
- King, J., & Stephan, A. (2021). Regulating privacy dark patterns in practice-drawing inspiration from california privacy rights act.
- Kollmer, T., & Eckhardt, A. (2023). Dark patterns: T. kollmer, a. eckhardt. *Business & Information Systems Engineering*, *65*(2), 201–208.
- Lalsinghani, G. (2024). Left in the dark: Evaluating the ftc’s limitations in combating dark patterns. *Berkeley Tech. LJ*, *39*, 1463.
- Leiser, M., & Santos, C. (2023). Dark patterns, enforcement, and the emerging digital design acquis: Manipulation beneath the interface.
- 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*, 1–18.
- Mulgund, P., Mulgund, B. P., Sharman, R., & Singh, R. (2021). The implications of the california consumer privacy act (ccpa) on healthcare organizations: Lessons learned from early compliance experiences. *Health Policy and Technology*, *10*(3), 100543.
- Nousiainen, K., & Perdomo Ortega, C. (2023). Dark patterns in law and economics framework. *Loy. Consumer L. Rev.*, *36*, 90.
- Santos, C. T., Bielova, N., & Gray, C. M. (2024). Two worlds apart! closing the gap between regulating eu consent and user studies. *Harvard Journal of Law & Technology*, *37*(3), 1295–1333.
- Shadikhodjaev, S. (2021). Technological neutrality and regulation of digital trade: How far can we go? *European Journal of International Law*, *32*(4), 1221–1247.
- 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.
- Solove, D. J. (2021). The myth of the privacy paradox. *Geo. Wash. L. Rev.*, *89*, 1.
- Sprague, R., & Wells, M. E. (2010). Regulating online buzz marketing: Untangling a web of deceit. *Am. Bus. LJ*, *47*, 415.
- Tran, V. H., Mehrotra, A., Sharma, R., Chetty, M., Feamster, N., Frankenreiter, J., & Strahilevitz, L. (2025). Dark patterns in the opt-out process and compliance with the california consumer privacy act (ccpa). *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, 1–25.
- U.S. Congress. (2023). Text - s.2708 - 118th congress (2023-2024): Detour act [Accessed: 2025-05-23]. <https://www.congress.gov/bill/118th-congress/senate-bill/2708/text>
- Van Deursen, A. J., & Helsper, E. J. (2015). The third-level digital divide: Who benefits most from being online? In *Communication and information technologies annual* (pp. 29–52, Vol. 10). Emerald Group Publishing Limited.
- Wilson, L. (2023). Is there a light at the end of the dark-pattern tunnel? *Geo. Wash. L. Rev.*, *91*, 1048.
- Witte, J., Kenning, P., & Brock, C. (2023). Consequences of user manipulation through dark patterns. *Proceedings of the Forty-Fourth International Conference on Information Systems (ICIS 2023)*, 10-13 December 2023, Hyderabad, India.
- World Health Organization. (2021). Ageing and health [Accessed: 2025-06-11].