Work-in-Progress: Uncovering Dark Patterns: A Longitudinal Study of Cookie Banner Practices under GDPR (2017-2024)

Zihan Qu*§, Xinyi Qu†§, Xin Shen*§, Zhen Liang*§ and Jianjia Yu*
*Johns Hopkins University
†University College London
zqu6@alumni.jh.edu, xinyi.qu.19@alumni.ucl.ac.uk, {xshen45, zliang30, jyu122}@jhu.edu

***Abstract*—This study investigates the evolution of cookie banner practices and the impact of General Data Protection Regulation (GDPR) frameworks on dark pattern behaviors across European Union (EU) and United Kingdom (UK) websites from 2017 to 2024. By examining predefined categories of dark patterns and analyzing Business-to-Business (B2B) and Business-to-Consumer (B2C) websites, the study reveals a significant decline in overt manipulative practices, such as "No Banner" and "Only Opt-In," following GDPR implementation. However, it identifies a substantial rise in subtler tactics, including "More Options," "Highlighted Opt-In," and "Preference Preselected," with a higher prevalence on B2C websites. The findings highlight the persistence of manipulative practices despite regulatory efforts and emphasize the need for ongoing refinement of privacy policies to address evolving strategies in cookie consent mechanisms.**

I. Introduction

At the core of data transmission on the Internet lies the use of cookies. Initially designed for simple session management, cookies have now evolved into complex tools for tracking and advertising. While enabling businesses to monitor user behaviors and implement targeted advertising, their widespread use raises significant privacy concerns regarding the collection, use, and sharing of personal information without explicit user consent.

In response, data protection regulations such as the General Data Protection Regulation (GDPR) [1] in the European Union (EU) and the California Consumer Privacy Act (CCPA) [2] in the United States (US) have been introduced. These regulations emphasize consent mechanism to empower user rights and have reshaped cookie practices. Despite these policies reducing online cookie tracking, transparency of cookie implementation and activation for user behavior analysis remains opaque to web visitors.

Existing literature primarily examines the impact of cookie tracking on privacy and online marketing within specific platforms, such as social media website [3], and new cookie banner designs that evolved from 6 dark pattern defined by GDPR [4], [5]. Trevisan et al. [6] revealed widespread non-compliance, with 49% of websites installing profiling cookies without user consent, highlighting enforcement challenges. Nouwens et al. [7] further exposed the prevalence of dark patterns, with only 11.8% of the examined UK websites meeting minimal European compliance standards. Building on these gaps, Jha et al. [8] demonstrated how subtle design changes significantly influence user consent decisions. However, there is limited longitudinal analysis of how dark patterns in cookie banners have evolved in response to regulatory changes over time [9], [10].

This study addresses this gap by employing longitudinal analysis (2017-2024) to compare pre- and post-GDPR cookie behaviors on the United Kingdom (UK) and EU web-pages using the Internet Archive database. It investigates how cookie banners have adapted to regulatory and technological changes, the strategies websites use to comply with or circumvent these regulations, and the emergence of so-called dark patterns, i.e., manipulative cookie banners to trick users to give consent for all cookies. Specifically, by examining the prevalence and evolution of various dark patterns in relation to GDPR and across different business settings, this study provides a broader understanding of digital ethics and compliance in an evolving regulatory landscape.

This research contributes to the discourse on digital privacy and user consent by evaluating cookie consent mechanisms and identifying the presence of dark patterns to assess the effectiveness of legislative and technological measures. It provides guidance for future decisions in Internet governance, privacy law, and web development. While the findings reveal a noticeable decrease in traditional manipulative cookie banners, they also highlight the emergence of more sophisticated and subtle techniques, complicating the regulatory environment. This emphasizes the need for website developers to adopt more transparent and user-respecting practices and for policymakers to refine regulatory frameworks to address these evolving challenges.

This paper is organized as follows: Section II defines the problem, Section III discusses background information, Section IV explains data collection and labeling methods, Section V describes the measurement framework of cookie banners, Section VI presents result analysis, and Section VII presents conclusion and limitation.

§Z. Qu, X. Qu, X. Shen, and Z. Liang assert joint first authorship.

Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb) 2025
28 February 2025, San Diego, CA, USA
ISBN 979-8-9894372-9-0
https://dx.doi.org/10.14722/madweb.2025.23016
www.ndss-symposium.org

II. Problem Definition

Cookies were originally designed to enhance user convenience by remembering login details, preferences, and other personalized settings across web sessions. However, the widespread use for tracking user behavior across websites has raised alarms regarding user privacy and potential risks of personal data misuse.

The GDPR was introduced to address these privacy challenge by providing users with greater control over their data and enforcing stricter guidelines on how businesses collect, store, and use information. A pivotal aspect of evaluating the impact of such regulations is examining how cookie banners have evolved in response. While these banners are intended to offer users a choice regarding cookie acceptance, many incorporate dark patterns that trick user into accepting all cookies, undermining the effectiveness of privacy regulations. The research aims to examine changes in the prevalence and nature of dark patterns over time, assessing the extent to which regulatory measures have curbed manipulative practices and enhanced user privacy.

III. Background

A. Privacy Regulation

The GDPR framework enhances personal data protection and strengthens the individual rights over their information. It serves as a comprehensive privacy law for the EU, setting standards for data processing, consent, access, deletion, and portability. GDPR applies to entities both within and outside the EU that handle data of EU residents, emphasizing transparency, security, and accountability and enforcing strict penalties for non-compliance.

B. GDPR Timeline

The implementation of the GDPR in May 2018 marked a regulatory shift, evolving through ongoing updates and guidelines issued by the European Data Protection Board (EDPB). This dynamic development reflects the increasing rigor in safeguarding user consent and addressing deceptive practices in digital environments.

Initially, GDPR prioritized obtaining user consent for cookie usage. However, unclear guidelines often led to practices like "cookie walls," which is a pop-up that restricts or blocks access to website until the user accepts the cookie usage. In 2020, following Brexit, the UK introduced its own version of GDPR (UK GDPR), requiring organizations to adapt data transfer mechanisms to comply with both EU and UK standards. Implied consent mechanisms, such as pre-ticked boxes or passive actions, were explicitly prohibited [11], [12].

Between 2020 and 2022, privacy concerns gained prominence [13]. In May 2020, the EDPB banned "cookie walls" and clarified that passive behaviors, like scrolling or swiping, do not constitute valid consent [14]. In 2022, addressing growing concerns about deceptive practices, the EDPB issued guidelines on dark patterns, identifying six primary types of manipulative website interfaces [15].

By 2023, the EDPB "Cookie Banner Taskforce" introduced stricter regulations for consent banners. Key requirements included equally display a reject button on the first layer, avoid pre-ticked boxes, ensure button colors and contrasts are not deceptive, refrain from relying on "legitimate interest" as the legal basis for processing personal data, provide a "withdraw consent" option, and the cookie banner should keep showing on each page until the visitor explicitly give consent [16]. However, the taskforce did not specify aesthetic design elements, such as color and contrast.

C. Analysis of Dark Patterns in Cookie Consent

Cookie consent dialogs often incorporates subtle manipulative techniques to nudge users into consenting to broader data processing than they might otherwise agree to. Coined by UX designer Harry Brignull in 2010, "dark patterns" are deceptive user interface designs that influence users choices presenting options in a biased manner [17].

The EDPB 2022 guidelines identified six deceptive practices - Overloading, Skipping, Stirring, Obstructing, Fickle patterns, and Left in the dark - as violations of GDPR [5]. These practices serve as fundamental criteria for determining if a cookie consent mechanism constitutes a dark pattern. Building on this foundation, Daniel Kirkman et al. [18] developed "Dark Dialogs", an analytical tool that isolates cookie consent dialogs from websites to identify prevalent dark patterns. They defined ten novel dark patterns, which will be referenced in this research to track and analyze results.

IV. Data Collection

A. Cookie Banner Consent Data Collection

The Wayback Machine, developed by the Internet Archive, serves as the primary data source for this research. It archives worldwide historical versions of web pages since 2010 [19]. Cookie banners, stored as part of the frontend content, can be extracted and analyzed for dark patterns. To efficiently retrieve data, the Waybackpy API is employed as an interface with the Wayback Machine database. To ensure regional consistency and compliance with EU regulations, websites or sub-websites specifically from the EU region, such as those with FR and GB domains, were selected from the globally crawled Wayback Machine.

The study focuses on websites with B2B (Business-to-Business) and B2C (Business-to-Consumer) models, as these sites rely heavily on personal data analysis for user profiling and personalized marketing. Such websites often deploy sophisticated cookie banner strategies, making them ideal for studying user interaction and consent mechanisms.

Snapshots were selected from mid-year, typically between May and July, to ensure a neutral and representative website appearance. If no banner was detected, the range was iteratively expanded to include adjacent months until a visible banner was identified. Moreover, only complete snapshots with HTTP status codes in the 2xx range are selected, ensuring accurate representation of the original content as it appeared at the time of capture [20].

B. Website Selection Process

Hundreds of websites from the Tranco list (updated December 2024) [21] were scanned, resulting in a final selection

of 100 websites that consistently featured cookie banners from at least 2020 to 2024. The selected websites represent top global companies across diverse sectors, ensuring a broad and representative sample for comprehensive analysis.

The selection process comprises two phases: Phase 1) Automatic Detection: An open source tool from the University of Edinburgh [18] is modified to enhance its detection capabilities for cookie banners, particularly against light backgrounds with minimal contrast. Phase 2) Human-labeled Correction: Snapshots are manually reviewed to classify them as containing or not containing cookie banners. For those with banners, each is categorized into one of the eight out of ten predefined dark pattern types by Daniel Kirkman et al. [18]. Additionally, potential novel dark patterns are identified. If they do not fall into the eight pattern types, we categorized them into new types, as demonstrated in section VII C.

C. Complexity of Cookie Consent Data Collection

Several challenges were encountered during data collection: 1) The Wayback Machine does not always preserve complete snapshots due to accessibility barriers, such as crawling restrictions [22]. Additionally, it only allows for the analysis of visual aspects of websites, limiting the ability to observe dynamic functionality as it would operate in real-time. To ensure relevance for analyzing cookie behaviors and regulatory compliance across distinct operational contexts, the selection focused exclusively on business websites. The classification of websites as B2B or B2C was based on publicly available information, where B2B refers to transactions between businesses, and B2C involves transactions between a business and an individual as the end customer [23]. 2) Misclassification of elements by the automated tool posed a risk to accuracy. To mitigate this, manual verification was performed to ensure accurate identification and categorization of cookie banners. This two-phase approach, combining automated detection and manual verification, ensures the reliability of the dataset for analyzing the evolution of cookie banners and their associated dark patterns.

V. Measurement Framework

This research aims to quantify the evolution and functionality of cookie banners over time to assess how these changes correspond to the guidelines of GDPR. The analysis focuses on the following dimensions:

1) Changes in Cookie Banner Appearance: Examine alterations in the design and visual presentation of cookie banners before and after GDPR implementation.

2) Disclosure of Cookie Usage: Assess whether websites have improved transparency in informing users about the use and purpose of cookies.

3) User Data Management Rights: Evaluate whether users are provided with clear and accessible options to manage their data effectively.

4) Visibility of Cookie Settings: Identify dark patterns that obscure cookie settings, such as nudging or redirecting users to separate pages, complicating the process of managing consent preferences.

VI. Results and Analysis

A. Analysis of the Cookie Consent Banner based on Dark Pattern Categories

Dark patterns in cookie consent are often combinations of six basic deception design patterns defined by EDPB. This analysis identifies six prevalent patterns [18]: Only Opt-In, Highlighted Opt-In, More Options, Complex Text, Ambiguous Close, and Preference Slider (Figure 8, Figure 1, Figure 2, Figure 9, Figure 10, Figure 11).

1) Only Opt-In: The "Only Opt-In" dark pattern falls under the categories of Skipping and Left in the Dark. This manipulative design tactic, as discussed by Sanchez-Rola et al. [24] and Degeling et al. [25], aims to steer users toward agreeing cookies without providing a clear or accessible option to reject them. Typically, the cookie consent interface offers only an "Accept" button, while the option to decline cookies is either absent, obscured, or significantly more effort-intensive. This design effectively limits user choice, compelling them to consent to cookies due to inconvenience or lack of alternatives.

In appendix Figure 8, there were above 80% banners "Only Opt-In" between 2017 and 2019. A notable decline followed the release of GDPR guidelines in 2020, which emphasized the importance of "freely given" consent, requiring that users have real choice and control over their consent. Consent is invalid if users are compelled, face negative consequences for refusal, or if rejecting consent is unreasonably burdensome [26]. More influential was France's data protection agency, CNIL, imposing fines on Google and Facebook for omitting a "reject all" button, signaling stricter enforcement and significantly reshaping cookie consent practices.

By 2020, many websites moved away from the Only Opt-In model, incorporating more comprehensive options such as "Reject All", "More Options", or "Custom Cookies". These changes reflect a shift toward compliance with GDPR's stricter requirements for user autonomy and transparency.

2) Highlighted Opt-In: The "Highlighted Opt-In" dark pattern falls under category of Stirring, where user interface design manipulates user behavior through visual emphasis. In this pattern, the opt-in button for cookies or consent forms intentionally feature a background color that is more prominent or visually appealing than the opt-out button. This visual distinction draws users' attention to the opt-in button, increasing the likelihood of consent without fully considering alternatives, such as declining. By leveraging human preference for visually attractive elements, this tactic subtly guides users toward decisions that may not align with their privacy preferences or intentions. The primary goal is to maximize user consent, often at the expense of informed choice and privacy.

In Figure 1, from 2017 to 2019, only a small number of websites employed this tactic. However, between 2019 and 2020, its adoption increased significantly, rising from 10% to 30%, reflecting a growing preference for emphasizing opt-in buttons through visual prominence. Following the peak, there was a slight decline as some websites began to remove this design to enhance clarity and compliance.

The GDPR guidelines on consent in 2020 emphasized the principle of "freely given" consent [27], requiring websites to

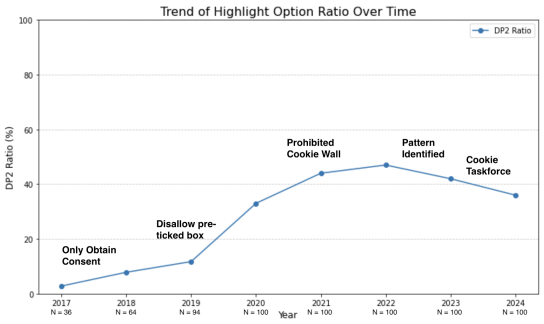


Fig. 1: Ratio of "Highlighted Opt-in" over all selected websites per year.

provide users with options beyond "Accept All". In response, many websites adopted "Highlighted Opt-In" to steer users toward "Accept All" by enhancing its visual appeal. By 2023, the second GDPR guidelines addressed Emotional Steering as a violation, targeting manipulative tactics that use visual or emotional elements - such as style, colors, and images - to influence user decisions, often against their own data protection interests [28].

Nevertheless, the effect on "Highlighted Opt-In" has been limited, as the usage of this pattern slightly decreased after 2020. The minimal impact is possibly due to ongoing debates about whether prominently displayed "Accept All" buttons constitute Emotional Steering.

3) More Options: The "More Options" dark pattern combines elements of Stirring and Fickle Interface. In this design, additional options for managing cookie consents are hidden behind a "More Options" button, while an easily accessible "Accept All" option is prominently displayed. By exploiting decision fatigue, this design increases the likelihood that users will accept all cookies to avoid the effort required to navigate multiple layers to decline or customize their preferences.

In Figure 2, from 2017 to 2019, this pattern was nearly absent, as noted by Sanchez-Rola et al. [24]. However, its adoption grew significantly from 2019 to 2023, rising from 5% to 55%, reflecting a growing preference for using hidden options to nudge users toward consent while making refusal or customization unnecessarily burdensome. After peaking in 2023, its use began to decline.

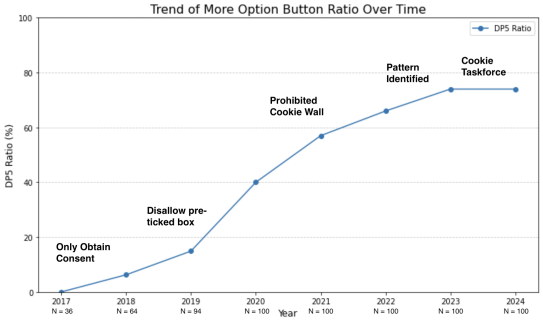


Fig. 2: Ratio of "More Options" over all selected websites per year.

The rise of the "More Options" dark pattern aligns with the first GDPR guidelines in 2020, which emphasized "freely given" consent [27]. By concealing options to decline cookies, websites attempted to maintain compliance while still steering users toward consent. However, the decline after 2023 corresponds to regulatory enforcement, such as the 150-million-euro fine imposed on Google LLC by CNIL for failing to provide clear and accessible options for declining cookies [29].

The second GDPR guidelines further addressed this issue by mandating that "Opt-Out" buttons be equally accessible on the first layer of cookie banners [16]. By 2024, many websites adjusted their designs to place Opt-In, Opt-Out, and More Options buttons on the same interface layer, reducing reliance on the More Options dark pattern.

4) Complex Text: Falling on the categories of Overloading and Obstructing, this design employs intricate and dense language in dialogue texts or consent forms. Characterized by technical jargon, lengthy sentences, and complex vocabulary, it obscures the implications of user consent, making it difficult for users to understand and make informed decisions. The convoluted text can confuse or overwhelm users, often resulting in unintentional consent to terms they might otherwise reject if the information were presented clearly and concisely.

In appendix Figure 9, between 2017 and 2021, its adoption steadily increased from 8% to 33%. As privacy regulations became enforceable, websites added more data collection details in cookie banners. However, some exploited this requirement by using dense language to confuse users, leading to uninformed consent. After 2021, its use fluctuated slightly, as websites rarely altered the content of their cookie consents once established.

Both GDPR guidelines stress providing users with clear and accessible privacy information. The 2020 guidelines require "unambiguous indication of wishes" through a clear statement or affirmative action [14]. In 2023, GDPR identified Obstructing as a deceptive design pattern and a violation of data protection regulations [28].

Despite these regulatory updates, the prevalence of Complex Text has not significantly declined. This persistence is attributed to the difficulty in objectively determining whether a text is overly complex. Tools like the Flesch-Kincaid (FK) reading ease test, which evaluates readability based on sentence length and syllable complexity, are used to assess cookie consent texts [30]. However, GDPR lacks a definitive standard for readability, allowing websites to maintain overly complex content in their cookie consents.

5) Ambiguous Close: Falling under the categories of Fickle and Left in the Dark, this dark pattern features a close button (often represented as an "X" or "Close") on cookie consent pop-ups, with unclear functionality. This ambiguity creates usability issues, potentially leading users to make unintended choices, such as inadvertently consenting to cookie tracking.

In appendix Figure 10, from 2017 to 2024, the percentage of websites using "Ambiguous Close" steadily decreased. Although not officially banned, countries like France require "Continue without accepting" as a close button on the notices. The 2023 GDPR guidelines classified "Hidden in Plain Sight" as a deceptive design pattern. The concept refers to presenting crucial data protection information in ways that make it easily overlooked by users, violating the transparency principle of GDPR, which mandates clarity and visibility in presenting information about personal data processing [28]. For the "Ambiguous Close", websites often include a "close" button without clearly indicating what cookie tracking rules will apply

after the user closes the consent pop-up. This practice can be interpreted as a violation of GDPR's "Hidden in Plain Sight" rule. Nevertheless, this dark patter remains common due to two factors. Firstly, the "Ambiguous Close" often appears alongside other dark patterns, reflecting immature cookie consent designs. Such designs are often found on lower-traffic websites, where limited operational impact reduces the incentive for compliance improvements. Secondly, the "Close" button is not prominent, having less severe implications compared to other dark patterns. While it may confuse users, it does not substantially hinder their ability to navigate or understand their choices.

6) Preference Slider: The "Preference Slider" dark pattern combines elements of Stirring, Fickle, and Left in the Dark. This pattern involves user interface elements, specifically sliders, being preset to an "enabled" position by default when users first encounter them. This pattern typically features multiple preference sliders, with some set to "on" by default. This design increases the likelihood of user error or oversight, potentially leading to unintentional consent. While sliders controlling "Necessary Cookies" (essential for website functionality) are excluded under this dark pattern if locked in an enabled state, all other sliders preset to "enabled" is subject to scrutiny due to their deceptive implication of consent.

In appendix Figure 11, its use in 2017 was negligible, as websites rarely provided detailed slider options for users at that time. Nevertheless, from 2018 on-wards, the adoption of this pattern steadily increased, rising from 5% to 22%, with some websites introducing specific sliders such as "marketing usage" or "increase customer performance".

Despite this growth, the Preference Slider remains uncommon. Many websites prefer using "Necessary Cookies" or placing slider options within the "More Options" layer rather than the first layer of cookie consent banners. The adoption of this pattern often varies by purpose. For example, B2C websites, which rely heavily on cookie data for personalization and advertising, often opt for the "Accept All" option instead of detailed slider configurations, as maximizing user consent aligns with their business model.

B. Comparative Analysis of the Cookie Consent Banner based on Business Models (B2B/ B2C Websites)

This section provides a comparative analysis of dark patterns on B2B and B2C websites over time, using key GDPR milestones as reference points: obtain consent required (2017 – 2018), prohibited cookie wall (2020 - 2022), and cookie banner taskforce (2022 – 2023). The analysis evaluates of regulations in addressing dark patterns. (In this section, "user" refers to an individual visiting a business company webpage as part of their role in a business department.)

1) No Banner and Consent Required: When GDPR began requiring cookie banner consent in 2017, both B2B and B2C websites exhibited a declining trend in the use of "No Banner". This indicates an initial response to regulatory demands for transparency (see Figure 12 in appendix). The introduction of GDPR in 2017, which required cookie banner consent, prompted a notable decline in the use of "No Banner" on both B2B and B2C websites. This indicates an initial response to regulatory demands for transparency.

2) Prohibited Cookie Wall: The prohibition of cookie walls in 2020 marked a significant GDPR milestone [14]. In appendix, Figure 13, B2C websites quickly reduced their use of cookie walls, prioritizing user experience and compliance, while B2B websites adapted more slowly. Nevertheless, B2B websites eventually aligned with GDPR principles, albeit with less urgency than their B2C counterparts. Both B2B and B2C websites keep low level of using cookie wall in 2024. Due to UK GDPR policy in disallowing pre-ticked box in the cookie banner, which push the websites owner display cookie options that indirectly reduce the "only opt-in" using and make both B2B and B2C show decline trends since 2019.

The prevalence of the "Ambiguous Close" pattern has remained relatively stable across years for both B2B and B2C websites (see Figure 17 in appendix). GDPR requires cookie banners to remain visible until users make a consent choice but does not explicitly prohibit the use of close buttons, leaving this issue unresolved [16].

3) Cookie Banner Taskforce: The introduction of the Cookie Banner Taskforce in 2023 aimed to address manipulative designs, but its impact on key patterns has been mixed:

In appendix Figure 16, the use of "Highlighted Opt-in" increased substantially after GDPR enforcement began, as companies sought alternative strategies to influence user consent decisions. This pattern became a preferred method for manipulating users, given its effectiveness. Despite the prohibition of cookie walls and taskforce regulations, its use has seen little reduction across both B2B and B2C websites. Notably, since 2020, B2B websites have relied on this pattern more than B2C websites, potentially due to differences in user demographics and engagement approaches.

The "More Options" dark pattern, often requiring users to navigate to a separate page to customise cookie preferences, has seen a dramatic increase since GDPR mandated user consent (see Figure 14 in appendix). This pattern is widely used in cookie banners with multiple consent options. Its persistent prevalence suggests that key regulations, including those requiring all cookie options to be displayed on the same page, as mandated by the taskforce, have been ineffective in curbing its use.

The "Preference Preselected" dark pattern is often associated with the use of the "More Options" strategy. In appendix Figure 15, following the adoption of the pre-ticked box regulation (2018-2020) and the emergence of the "More Options" dark pattern, companies shifted from using pre-ticked boxes to using "More Options" pages to obscure analytical and marketing cookies reselected by default. A steady increase in the use of this pattern have been observed on both B2B and B2C websites since 2019. While the cookie taskforce regulation discouraged highlighted options, leading to a slight decline on B2C websites, both categories show an overall upward in employing "Preference Preselected" strategies.

In examining "Preference Preselected," "More Options," and "Highlighted Opt-In" collectively (see Figure 3 in appendix), B2C websites consistently demonstrate faster growth and higher usage rates of these patterns compared to B2B websites. This trend highlights the greater prevalence of manipulative designs in B2C environments, driven by their focus on consumer interactions.

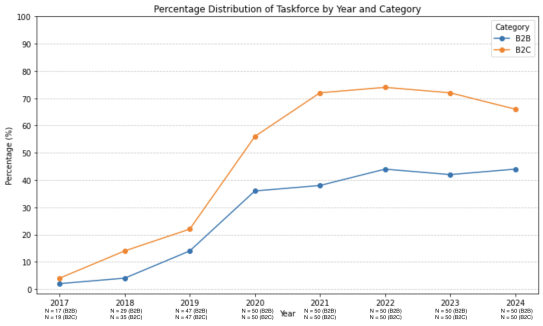


Fig. 3: Use of dark pattern in "Taskforce 2023" distribution over time (B2B vs. B2C).

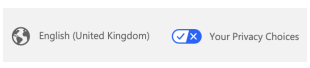
A closer examination reveals that "Highlighted Opt-In" frequently coexists with "More Options" buttons, with the latter often used to conceal cookie configurations on secondary layers (see Figure 3 in appendix). Existing studies [4] support this finding, showing that the absence of in-line cookie alternatives on the first screen encourages users to accept all cookies, undermining informed decision-making. By combining visually prominent opt-in options with hidden configuration layers, these patterns diminish user autonomy, reduce engagement with granular privacy settings, and prioritize data collection.

4) Contextual Factors Influencing Dark Patterns: Financial-services-based companies usually carefully collect data and pay more attention to stepping up privacy requirements [31]. For such companies, leveraging privacy compliance can create a business advantage. Hogsbro [32] highlights that data protection is key to customer trust, not just compliance. B2B companies are generally more cautious about data collection, avoiding manipulative practices, for example, the "Accept All" button, to maintain strong relationships with individual customers. In contrast, B2C websites may prioritize user convenience over privacy, which could explain the higher prevalence of highlighted opt-in patterns.

C. Preliminary Findings Beyond Prior Work

This section identified three unregulated dark patterns that hinders users in navigating cookie consent mechanisms.

1) Unnoticeable Privacy Collection Icon/Banner: In Figure 4, Subfigure 4a, this dark pattern features an inconspicuous cookie banner placed at the bottom of the webpage with unconventional icons -a checkmark and a cross- smaller than the language selection button. Their functions are only revealed on mouse-hover. After clicked the icon, in Figure 4, Subfigure 4b, cookie tracking is enabled by default, potentially bypassing EDPB regulations, since website owner has stated that it complies with GDPR [33]. This pattern blends "Only Opt-in'and "Cookie Wall" tactics, collecting user data without transparent disclosure.



(a) Unconventional banner

(b) Privacy collection

Fig. 4: Unnoticeable privacy collection.

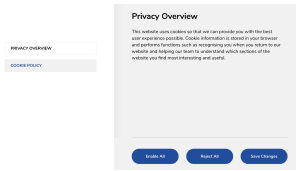
2) Vague Background Color Mixed with Webpage Background: This dark pattern uses ambiguous background colors and contrasts, blending the cookie banner into the page design. In Figure 5, the "Accept" button is deceptively integrated into the webpage, with text on cookie collection minimized to resemble copyright notices, reducing its visibility. The banner presents only a "Continue" button, which, when selected, assumes consent for all cookies without providing opt-out options, violating GDPR mandates.

Fig. 5: Vague background.

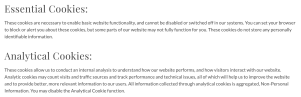
3) Partially Satisfied with Cookie Banner Taskforce with Unconfigurable forced action: This dark pattern involves a misleading "More option" interface that limits user configuration. In Figure 6, the banner only offers "Accept All" or "Reject All" without clearly specifying cookie types.

Fig. 6: Partially satisfied with cookie banner taskforce.

In Figure 7, Subfigure 7a, the adjacent "Save Changes" button opens a new window without clarifying cookies types. Users learn about analytical and essential cookies only by accessing the "Cookie Policy" within this window.



(a) Second page



(b) Cookie setting

Fig. 7: Cookie settings.

In Figure 7, Subfigure 7b, the option to select cookies remains opaque, with the selection of analytical cookies appearing to be mandatory.

VII. Limitation and Conclusion

This study highlights the significant and multifaceted impact of GDPR on cookies governance. While overt manipulative practices like "No Banner" and "Only Opt-In" have declined, subtler dark patterns such as "More Options" and "Complex Text" persist. These findings emphasize the need for continuous refinement of privacy regulations to address increasingly sophisticated manipulative designs.

This study has limitation on data collection, as the US-based Internet Archive may lack crawls in UK or EU, potentially misrepresenting dark patterns in the EU and UK. Future research should prioritize regional web archives, such as EU and UK web archive, and cross-validate with the Internet Archive for greater accuracy and mitigate unrepresentative data.

Future research should explore diverse website categories and assess regional privacy regulations beyond GDPR to enhance global data protection policies. These insights can help policymakers address emerging challenges and strengthen user privacy protections across digital contexts.

References

[1] EUR-Lex, "Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation)," 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[2] CCPA, "California consumer privacy act of 2018," 2016. [Online]. Available: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

[3] Y. Dimova, G. Franken, V. Pochat, W. Joosen, and L. Desmet, "Tracking the evolution of cookie-based tracking on facebook," 11 2022, pp. 181–196.

[4] H. Habib, M. Li, E. Young, and L. F. Cranor, ""okay, whatever": An evaluation of cookie consent interfaces." ACM Conference, 2022.

[5] EDPB, Mar 2022. [Online]. Available: https://www.edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf

[6] M. Trevisan, S. Traverso, E. Bassi, and M. Mellia, "4 years of eu cookie law: Results and lessons learned," Jan 2019. [Online]. Available: https://dx.doi.org/10.2478/popets-2019-0023

[7] M. Nouwens, I. Liccardi, M. Veale, D. Karger, L. Kagal, A. Midas NouwensAarhus University Massachusetts Institute of Technology, C. Ilaria LiccardiMassachusetts Institute of Technology, L. Michael VealeUniversity College London, C. David KargerMassachusetts Institute of Technology, and C. Lalana KagalMassachusetts Institute of Technology, "Dark patterns after the gdpr: Scraping consent pop-ups and demonstrating their influence: Proceedings of the 2020 chi conference on human factors in computing systems." 2020 CHI Conference on Human Factors in Computing Systems, Apr 2020. [Online]. Available: https://dl.acm.org/doi/10.1145/3313831.3376321?utm_source

[8] N. Jha, M. Trevisan, M. Mellia, D. Fernandez, and R. Irarrazaval, "Privacy policies and consent management platforms: Growth and users' interactions over time," 2024. [Online]. Available: https://arxiv.org/abs/2402.18321

[9] A. Dabrowski, G. Merzdovnik, J. Ullrich, G. Sendera, and E. Weippl, "Measuring cookies and web privacy in a post-gdpr world," in *Passive and Active Measurement*, D. Choffnes and M. Barcellos, Eds. Cham: Springer International Publishing, 2019, pp. 258–270.

[10] M. Kretschmer, J. Pennekamp, and K. Wehrle, "Cookie banners and privacy policies: Measuring the impact of the gdpr on the web," vol. 15, no. 4. New York, NY, USA: Association for Computing Machinery, jul 2021.

[11] May 2023. [Online]. Available: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/consent/

[12] ICO, accessed: Jan. 2025. [Online]. Available: https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/the-uk-gdpr/

[13] EDPB, 2021. [Online]. Available: https://edpb.europa.eu/system/files/2022-05/edpb_2021_executive_summary_en.pdf

[14] ——, May 2020. [Online]. Available: https://www.edpb.europa.eu:443/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

[15] ——, Feb 2023. [Online]. Available: https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf

[16] ——, Jan 2023. [Online]. Available: https://www.edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf

[17] H. Brignull, "Dark patterns: Deception vs. honesty in ui design," 2011. [Online]. Available: https://alistapart.com/article/dark-patterns-deception-vs.-honesty-in-ui-design

[18] D. Kirkman, K. Vaniea, and D. W. Woods, "Darkdialogs: Automated detection of 10 dark patterns on cookie dialogs," in *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*. IEEE, 2023, pp. 847–867.

[19] Alexis, Oct 2010. [Online]. Available: https://archive.org/details/widecrawl?tab=about

[20] B. Kahle and B. Gilliat. Internet Archive, Sep 2013. [Online]. Available: https://archive.org/help/wayback_api.php

[21] V. L. Pochat, T. V. Goethem, S. Tajalizadehkhoob, M. Korczyński, and W. Joosen. Tranco, July 2024. [Online]. Available: https://tranco-list.eu/

[22] B. Kahle and B. Gilliat. Internet Archive, 2024. [Online]. Available: https://help.archive.org/help/wayback-machine-general-information/

[23] E. Heaslip, "B2b vs b2c: What's the difference?" Sep 2024. [Online]. Available: https://www.uschamber.com/co/start/strategy/b2b-vs-b2c

[24] I. Sanchez-Rola, M. Dell'Amico, P. Kotzias, D. Balzarotti, L. Bilge, P.-A. Vervier, and I. Santos, "Can i opt out yet? gdpr and the global illusion of cookie control," in *Proceedings of the 2019 ACM Asia conference on computer and communications security*, 2019, pp. 340–351.

[25] M. Degeling, C. Utz, C. Lentzsch, H. Hosseini, F. Schaub, and T. Holz, "We value your privacy... now take some cookies: Measuring the gdpr's impact on web privacy," 2018.

[26] Jan 2022. [Online]. Available: https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf

[27] Aug 2024. [Online]. Available: https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf

[28] GDPR. GDPR.eu, Sep 2023. [Online]. Available: https://gdpr.eu/article-15-right-of-access/

[29] "Closure of the injunction issued against google," Commission nationale de l'informatique et des libertés, 2023. [Online]. Available: https://www.cnil.fr/en/closure-injunction-issued-against-google

[30] J. P. Kincaid, R. P. Fishburne Jr, R. L. Rogers, and B. S. Chissom, "Derivation of new readability formulas (automated readability index, fog count and flesch reading ease formula) for navy enlisted personnel," 1975.

[31] V. Anant, L. Donchak, J. Kaplan, and H. Soller, "The consumer-data opportunity and the privacy imperative." McKinsey Company, Apr 2020. [Online]. Available: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative

[32] S. Høgsbro. Mono Solution, Aug 2021. [Online]. Available: https://www.monosolutions.com/b/why-online-businesses-should-care-about-their-website-cookies

[33] [Online]. Available: https://learn.microsoft.com/en-gb/legal/gdpr

Appendices

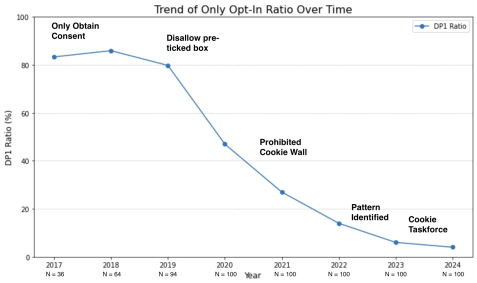


Fig. 8: Ratio of "Only Opt-In" over all selected websites per year.

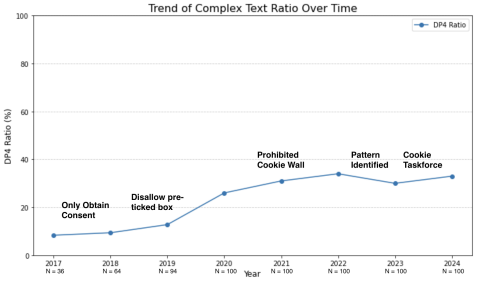


Fig. 9: "Complex Text" ratio over all selected websites per year.

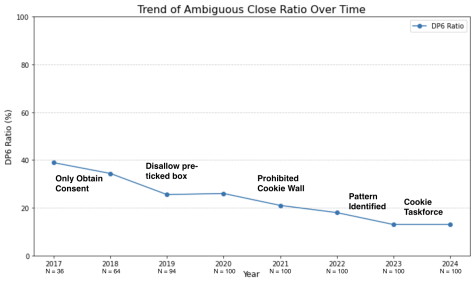


Fig. 10: “Ambiguous Close” ratio over all selected websites per year.

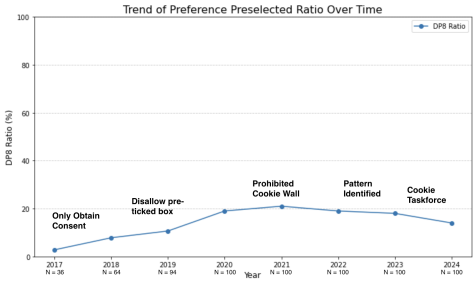


Fig. 11: “Preference Slider” ratio over all selected websites per year.

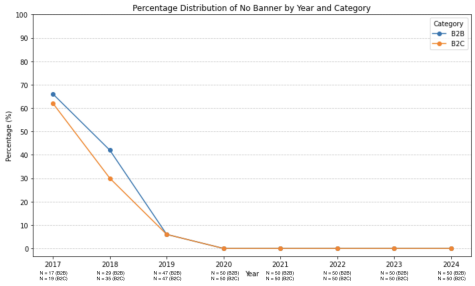


Fig. 12: “No Banner” distribution over time (B2B vs. B2C).

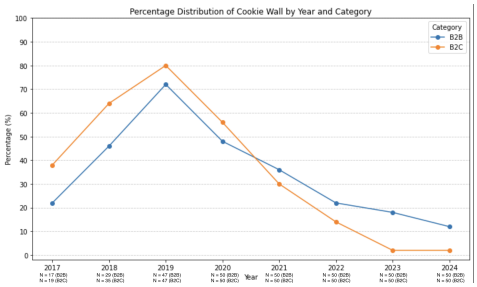


Fig. 13: Use of “Cookie Wall” distribution over time (B2B vs. B2C).

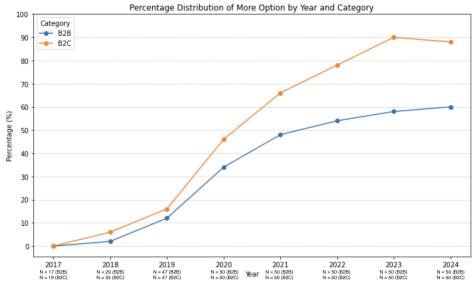


Fig. 14: “More Option” distribution over time (B2B vs. B2C).

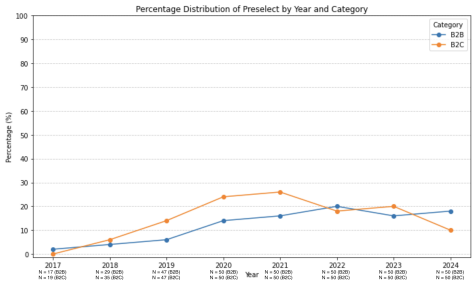


Fig. 15: “Preference Preselect” distribution over time (B2B vs. B2C).

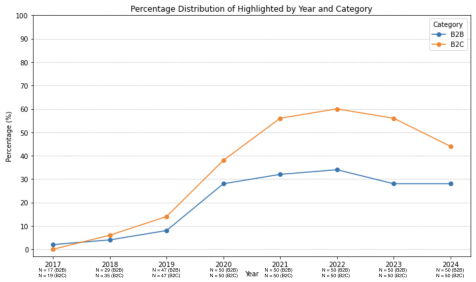


Fig. 16: “Highlighted Opt-in” distribution over time (B2B vs. B2C).

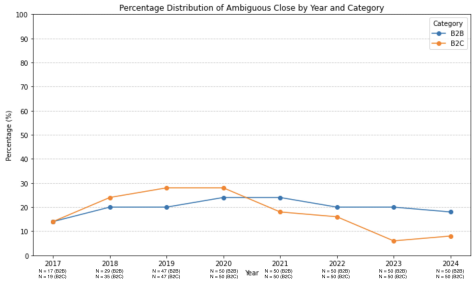


Fig. 17: “Ambiguous Close” distribution over time (B2B vs. B2C).