DIGITAL DECEPTION AND THE ILLUSION OF CHOICE: HOW DARK PATTERNS UNDERMINE INFORMED CONSENT DESPITE GDPR

A Paper
Submitted to the Graduate Faculty
of the
North Dakota State University
of Agriculture and Applied Science

By

Wajeeha Khan

In Partial Fulfillment of the Requirements
for the Degree of
MASTER OF SCIENCE

Major Program:
Software and Security Engineering

November 2023

Fargo, North Dakota

North Dakota State University

Graduate School

Title

DIGITAL DECEPTION AND THE ILLUSION OF CHOICE: HOW DARK PATTERNS UNDERMINE INFORMED CONSENT DESPITE GDPR

By

Wajeeha Khan

The Supervisory Committee certifies that this ***disquisition*** complies with North Dakota State University's regulations and meets the accepted standards for the degree of

MASTER OF SCIENCE

SUPERVISORY COMMITTEE:

Muhammad Zubair Malik

Chair

Zahid Anwar

Maria Alfonseca

Approved:

11/15/2023

Date

Simone Ludwig

Department Chair

ABSTRACT

Our investigation builds on prior research to examine global e-commerce data privacy, focusing on compliance with GDPR and CCPA laws introduced in 2018 and 2020. This study reveals uneven adherence to GDPR and CCPA regulations across e-commerce platforms, underscoring the persistent use of dark patterns. UK and French sites lead in GDPR compliance at 85% and 80%, while U.S. sites showed 65% adherence to CCPA. Turkish websites displayed a surprising 85% - 95% compliance with European standards. In contrast, South African platforms showed a low 30% compliance, often utilizing implicit consent methods. These findings expose significant gaps and inconsistencies in the application of data privacy laws across continents and nations. We advocate for a global standardization of data protection regulations to protect consumers and create a level playing field for businesses in the digital marketplace.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION

E-commerce is revolutionizing the traditional retail landscape, rapidly becoming the preferred method for shopping. As consumer behavior evolves, online purchasing is increasingly becoming the standard way to shop. The pandemic has undeniably influenced how people shop, steering more consumers towards online platforms for their purchases, ranging from groceries and food to clothing and other necessities. As e-commerce rapidly gains traction, transforming both traditional retail landscapes and consumer shopping habits, a plethora of challenges emerge in its wake. A key concern is the issue of security and privacy, which has become increasingly complex in the digital age. Nearly 27% of the global population is now engaged in online shopping, a setting where personal information is regularly exchanged (Vijayan 2019; Fokina 2023). The high stakes involved in protecting this sensitive data cannot be overstated.

Some e-commerce platforms employ dark patterns, and manipulative user interface designs aimed at tricking consumers into sharing more personal information than they may intend to (Di Geronimo et al. 2020; Gray et al. 2018; Nevala 2020). These deceptive tactics are often subtle, perhaps designed to resemble regular website features, making them even more insidious. They exploit the user's interaction with the site to extract personal data, sometimes without the user's clear understanding or consent. As such, dark patterns not only compromise individual privacy but also erode trust in the online shopping environment (Rust, Kannan, and Peng 2002; Shamsudhin and Jotterand 2022).

The introduction of regulatory frameworks like the General Data Protection Regulation (GDPR) in the European Union (Regulation 2018), the California Consumer Privacy Act (CCPA) in the United States (Goldman 2020), the Personal Information Protection Act (PIPA) in South Korea (Ko et al. 2017; "Statutes of the Republic of Korea" n.d.), Personal Information Protection

Law (PIPL) in China (Economy 2010; Calzada 2022) among other global privacy laws marks a significant milestone in the quest for enhanced digital privacy and security. These laws were specifically designed to give consumers more control over their personal data and to hold organizations accountable for how they handle this sensitive information. Significantly, the GDPR emerged as one of the first and most impactful of these regulatory frameworks, serving as a model for later privacy laws (Phillips 2018).

Under GDPR and CCPA, companies are obligated to follow strict rules about data collection, storage, and sharing. Failure to comply can result in substantial fines, which can reach up to 4% of a company's annual global turnover under GDPR or $2,500 to $7,500 per violation under CCPA (Kessler 2019; Wong, Chong, and Aspegren 2023). These penalties have been effective in compelling many websites and online services to adopt more transparent and responsible practices. For instance, these laws have led to the widespread adoption of Consent Management Platforms (CMPs), designed to solicit explicit consent from users about the types of data being collected and the purposes for which it will be used (Kessler 2019). The Consent Management Platform (CMP) typically has three main components in its user interface (Nouwens et al. 2020a):

- Initial Consent Page: This is the first screen users see, which outlines the general reason for the pop-up and presents overarching consent options such as 'accept all' or, in some cases, 'reject all' as shown in Figure 1 (a and b).
- Detailed Consent Page: This second screen delves into more specific data processing categories like personalization and marketing. It provides users with the ability to toggle these settings on or off, either individually or collectively, and features a button to submit the chosen consent preferences.

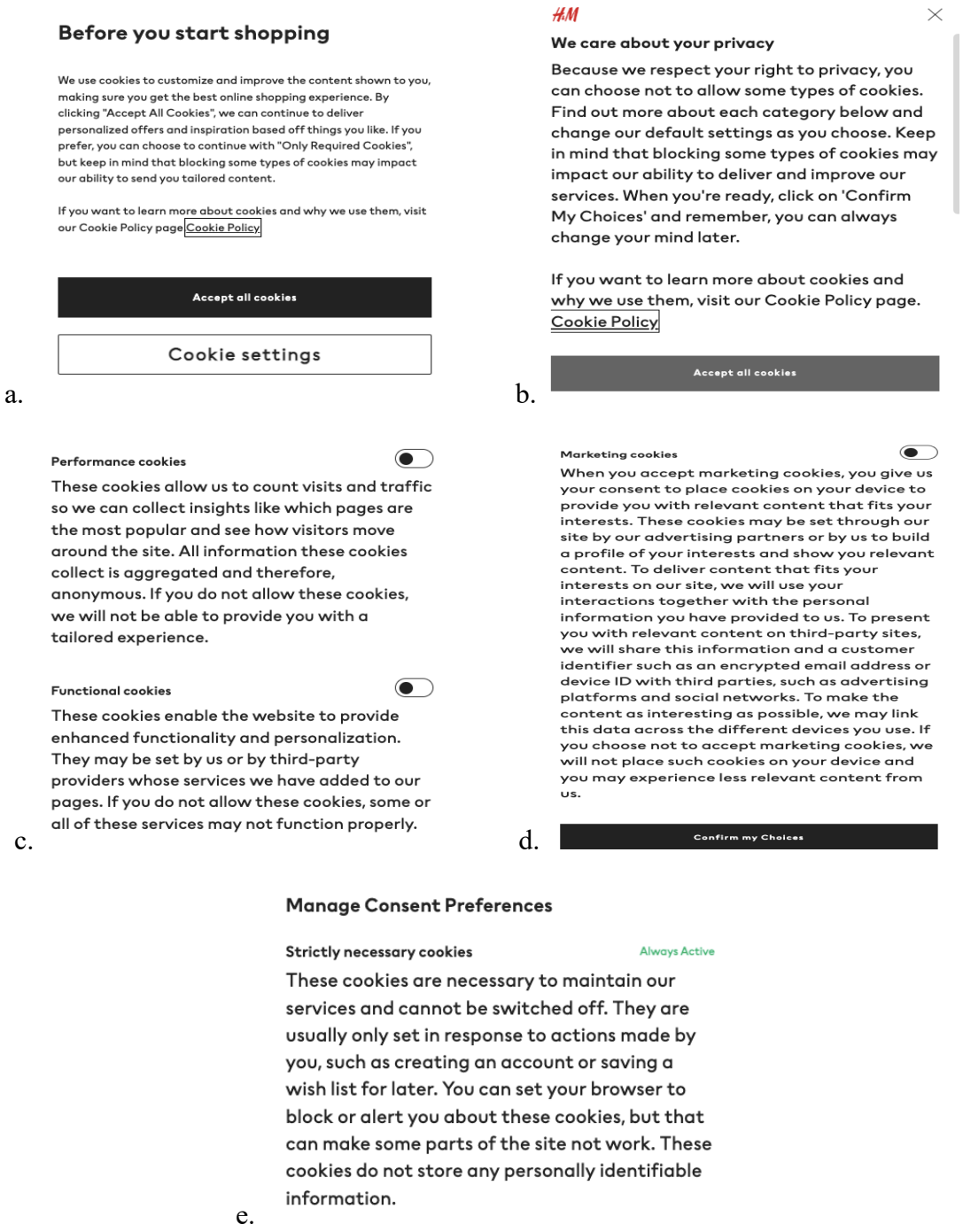

Figure 1. The three components of CMPs.

Note: The initial consent pages are represented in a and b. The detailed and vendor consent pages are represented in c, d and e. Screenshots sourced from https://www2.hm.com/en_us/index.html

- Vendor List Page: The final component lists all the third-party vendors who will be collecting or sharing data. This page also provides toggles to give or revoke consent for each vendor, individually or in bulk, along with a button to save these settings. (Figure 1 (b and c))

It should be noted that not all CMPs include each of these elements in their interface. However, the journey toward comprehensive digital privacy is far from complete. Despite the existence of these stringent laws, concerns are growing that some websites are still employing manipulative techniques known as 'dark patterns' to influence user behavior. These dark patterns are designed to deceive or coerce users into granting permissions or taking actions they might not fully understand or agree with. They can appear in the form of misleading language, hidden options, or confusing layouts, among other tactics, and they can be particularly prevalent in CMPs, where they can manipulate users into giving consent under ambiguous or misleading circumstances (Bongard-Blanchy et al. 2021a; Maier 2019).

2. RELATED WORK

In the realm of online privacy and data collection, various studies have explored the use of dark patterns, and manipulative design choices intended to influence user behavior, particularly in obtaining consent for data collection. These design choices continue to be effective in nudging users into relinquishing personal information without clear, informed consent, despite the implementation of the General Data Protection Regulation (GDPR) in 2018 (Soe et al. 2020; Nouwens et al. 2020b).

Further complicating this landscape are Consent Management Platforms (CMPs), which are increasingly employed by websites to manage user consent. These platforms often come with default settings that violate GDPR principles and engage in dark patterns. For instance, research indicates that 60% of default notices from major CMPs contain at least one dark pattern (Stöver et al. 2022). Another study involving two major CMP providers in the EU concludes that CMPs themselves process personal data and can act as controllers (Santos et al. 2021).

Researchers have also empirically evaluated the effectiveness of dark patterns. One study examined 53,000 product pages from 11,000 shopping websites and found 1,818 instances of dark patterns, categorizing them into 15 types and seven broader categories. Recommendations for mitigating the use of these patterns were also provided (Mathur et al. 2019). According to the literature, a two-stage usability assessment of cookie consent interfaces revealed that a fully-blocking consent interface with in-line options and a persistent button for later changes best serves user needs (Habib et al. 2022).

The issue extends beyond dark patterns and includes general compliance with privacy laws. For example, one study used PrivacyCheck, a data mining tool, to analyze 550 privacy policies for GDPR compliance and found significant gaps, particularly in transparency and the ability of users

to control their personal data (Zaeem and Barber 2020). In addition, there is a system called DarkDialogs, that automatically extracts and classifies dark patterns from consent dialogs on websites, showing that these patterns are prevalent regardless of the website's popularity or use of third-party CMPs (Kirkman, Vaniea, and Woods 2023).

On the user side, awareness of dark patterns does not necessarily translate into effective resistance. A survey involving 406 individuals showed that while users are generally aware of the manipulative influence of dark patterns, this awareness does not equip them with the tools to oppose such influence, especially among younger users (Bongard-Blanchy et al. 2021b).

Furthermore, the scholars on dark patterns reflect a variety of thematic and normative considerations [ref]. Research has incorporated perspectives from psychology, economics, ethics, philosophy, and law to provide a more holistic view of the implications and possible countermeasures against dark patterns (Mathur, Kshirsagar, and Mayer 2021). An investigation that focuses on the unethical design choices prevalent in five popular CMP services. They argue that these choices not only mislead users but also put website publishers in a precarious position regarding legal compliance (Toth, Bielova, and Roca 2022).

In the rapidly evolving e-commerce landscape, the urgency for ethical data practices is more critical than ever. E-commerce websites often hold vast troves of user data, which can be both an asset and a liability. Given the surge in the use of such websites globally, understanding and adhering to privacy regulations like the General Data Protection Regulation (GDPR) is not just a legal imperative but also a trust-building measure between businesses and their consumers. Our study aims to fill a significant gap in this area by scrutinizing the data collection practices across various e-commerce platforms. Importantly, our data is collected from multiple continents, offering a comprehensive look at how GDPR and similar policies are followed—or not—globally.

This international scope allows us to provide unique insights into the complexities of data privacy compliance in a world where online shopping knows no borders.

As far as GDPR standards are concerned, consent is a cornerstone for lawful data collection and processing. The regulation lays out specific criteria for obtaining valid consent: it must be freely given, informed, specific, and unambiguous (Rantos et al. 2019). In addition, users should be able to revoke their consent as easily as they gave it. Organizations are also required to document how and when consent was obtained. For sensitive types of data, explicit consent is often required, usually in the form of a clear written or spoken statement. These standards set the bar high, aiming to empower users to control their personal data and make informed decisions about how their data is used [GDPR].

Our study aims to assess how well e-commerce websites meet these GDPR standards, especially given the rise in e-commerce activity. By doing so, we hope to contribute to a more ethical e-commerce environment where both businesses and consumers can interact more transparently and securely.

3. METHODOLOGY

This research aimed to investigate how various e-commerce websites from different countries manage user consent for cookies, primarily considering GDPR compliance and the potential use of dark patterns. The study followed a systematic methodology to gather, analyze, and interpret the data.

3.1. Selection of Websites and Countries

The first step involved identifying e-commerce websites of interest from five countries: South Africa, the United Kingdom, Turkey, France, and the United States. The countries were selected to provide a diverse representation of different continents and legal jurisdictions, while the websites were selected based on their popularity and significance in the local e-commerce landscape.

3.2. VPN Setup

To ensure that the user experience of a local visitor was accurately replicated, a VPN (Virtual Private Network) was used. NordVPN was selected for this task. By routing the connection through a server in the respective countries, it was ensured that the websites would serve content and settings as they would to a typical user in those countries.

3.3. Collection of Data

The data collection process was carried out meticulously and involved visiting each website individually to examine and record how they handled cookie consent. The collected information included:

- **Implicit Consent:** It was noted whether the website assumes consent unless the user actively opts out, a practice that generally violates the GDPR rules requiring explicit consent (Spece Jr, Hilton, and Younggren 2016).

- **Explicit Consent:** Websites were checked for mechanisms that require an active indication of consent from the user, a GDPR requirement.
- **Consent Buttons:** The types of options presented to users to manage their consent were recorded, such as "Accept All", "Cookie Settings", or "Reject All".
- The types of buttons determine the level of control users have over their data. For example, having a "Reject All" button alongside an "Accept All" button offers clear choices. The buttons should facilitate informed consent, meaning that they should make it easy for users to understand what they are agreeing to and to say yes or no in an explicit manner**.**
- Depending on how they are implemented, buttons can either make a website GDPR-compliant or subject it to penalties.
- **Pre-ticked Choices:** The presence of pre-ticked boxes, which are generally not GDPR-compliant, was noted. Pre-ticked boxes are often seen as a way of gaining implicit consent, where the user is assumed to have agreed to the terms unless they actively opt out. This is generally not compliant with GDPR, which mandates that consent must be explicit. A pre-ticked box compromises user autonomy by making the decision for them, rather than allowing them to make an informed choice. This also violates the GDPR is requirement that consent be "freely given."
- **Banner Style:** Observations were made regarding the location and design of the cookie consent banner, i.e., whether it is presented in the footer of the website, or as a pop-up. The banner style and position have a significant impact on user interaction and consent, primarily because they govern how readily the information is presented and accessed.

The more visible and straightforward the banner is, the easier it is for users to make an informed decision. Here is why the banner's position matters:

1. **User Attention**: Where the banner is placed can dictate how quickly it captures user attention. A banner in a prominent location will not be easily missed and can prompt quicker interaction.
2. **User Experience**: The banner's position should be chosen to balance the need for attention without being overly obtrusive. An overly intrusive banner can disrupt the user experience, whereas one that is too subtle can get ignored.
3. **Ease of Interaction**: The banner's position can also affect how easily a user can interact with it to give or withdraw consent. If it is located in a hard-to-see or hard-to-reach place, the user might miss the opportunity to give informed consent, potentially making the website non-compliant with GDPR.

- **Use of Language:** The clarity and understandability of language in the consent banners were assessed. This is particularly important as GDPR requires the information about data collection to be transparent, intelligible, and easily accessible.

3.4. Data Analysis

Each website's information was organized into a table to facilitate comparison and analysis. The collected data was analyzed with respect to GDPR regulations and the presence of dark patterns. The compliance of each website with GDPR requirements was gauged based on the presence of explicit consent options, absence of pre-ticked choices, and clarity of the language used. Similarly, the potential use of dark patterns was investigated, based on how straightforward or deceptive the consent process appeared.

3.5. Documentation

Finally, the findings were documented, and interpretations were drawn based on the analyzed data. The differences in compliance levels across different countries and the use of dark patterns were noted, and an explanation of these findings was drafted.

This rigorous methodology ensured an in-depth and comprehensive understanding of how these e-commerce websites are managing user consent, particularly in relation to GDPR compliance and dark patterns. It is a repeatable process, allowing for ongoing monitoring of practices and trends over time.

4. FINDINGS

The findings from this research offer a rich, multi-faceted understanding of how e-commerce websites from five different countries i.e., South Africa, the United Kingdom, Turkey, France, and the United States manage cookie consent, with particular attention to GDPR compliance and the use of dark patterns. Below are the detailed findings for each country:

4.1. South Africa

In the South African context, it was observed that most websites did not comply with GDPR requirements. Most of the sampled sites, such as 'bobshop.co.za,' 'takealot.com,' 'zando.co.za,' 'everyshop.co.za,' and 'edgars.co.za,' were found to have no consent buttons as shown in Table 1. This is noteworthy because it implies a form of implicit consent, which is generally not compliant with GDPR rules that require explicit user approval for data collection.

Even more concerning is the complete absence of any option for users to customize their cookie settings, effectively taking the choice out of their hands. While GDPR is a European regulation, the best practices it outlines are increasingly considered the gold standard for user data protection worldwide. South African websites' apparent lack of mechanisms for explicit consent could pose problems, particularly for international users or in the future if South Africa adopts similar data protection laws.

Table 1. South African Website Evaluation

Website	Implicit Consent	Explicit Consent	Consent Buttons	Presence of Pre-Ticked Choices	Banner Style	Use of Language
https://www.bobshop.co.za/	✓		None	X	Website Footer	X
https://www.mrpricegroup.com/		✓	Accept All/ Cookie Settings	X	Website Footer	Clear
https://cottonon.com/ZA/	✓		None	X	X	X
https://www.takealot.com/	✓		None	X	Website Footer	X
https://www.zando.co.za/	✓		None	X	Website Footer	X
https://www.everyshop.co.za/	✓		None	X	Bottom Left	X
https://www.edgars.co.za/	✓		None	X	Website Footer	X

4.2. United Kingdom

The UK, being a part of Europe until recently, generally showed better compliance with GDPR. Websites like 'boohoo.com,' 'matalan.co.uk,' and 'amazon.co.uk' provided explicit consent options through buttons like "Let me choose," "Accept All," or "Customize Cookies" as shown in Table 2. However, it is worth mentioning that some websites still include pre-ticked boxes, which are generally not compliant with GDPR.

Table 2. United Kingdom Website Evaluation

Website	Implicit Consent	Explicit Consent	Consent Buttons	Presence of Pre-Ticked Choices	Banner Style	Use of Language
https://www.boohoo.com/		✓	Let me choose /Accept All	X	Website footer	Clear
https://www.matalan.co.uk/	✓		Accept	X	Website footer	Clear
https://www.selfridges.com/GB/en/		✓	Manage cookies/ Accept All	✓	Website footer	Clear
https://www.next.co.uk/		✓	Accept all/ Manually manage	✓	Pop -up	Clear
https://www.very.co.uk/		✓	Cookie Settings/ Accept all	X	Pop -up	Clear
https://www.newlook.com/uk		✓	Cookie Settings/ Agree	X	Bottom Left	Clear
https://www.amazon.co.uk/		✓	Accept/ Customize Cookies	X	Website footer	Clear

The use of language was also clear and understandable, giving users an easier path to make informed decisions. The adoption of these practices indicates a higher level of maturity and compliance with data protection regulations, although there is still room for improvement.

4.3. Turkey

Turkish e-commerce sites like 'trendyol.com,' 'hepsiburada.com,' and 'amazon.com.tr' generally provided options for users to give explicit consent through buttons labeled with terms like "Settings," "Admit it," and "Cookie Settings." This complies well with GDPR requirements for explicit consent, although, like the UK sites, some had pre-ticked choices, which could be seen as a dark pattern as shown in Table 3. The language used was clear, and the consent options were usually located in the website footer, making them relatively easy to find but not as immediately noticeable as a pop-up would be.

Table 3. Turkey Website Evaluation

Website	Implicit Consent	Explicit Consent	Consent Buttons	Presence of Pre-Ticked Choices	Banner Style	Use of Language
https://www.trendyol.com/		✓	Settings/ Admit it	X	Website footer	Clear
https://www.hepsiburada.com/magaza/gitti-gidiyor		✓	Cookie settings/ Admit it	X	Website footer	Clear
https://www.amazon.com.tr/		✓	Accept Cookies/ Customize Cookies	X	Website footer	Clear
https://www.ipekyol.com.tr/		✓	Settings/ Reject / Admit it	X	Website footer	Clear
https://www.boyner.com.tr/		✓	Admit it/ Cookie Settings	X	Bottom Right	Clear
https://www.migros.com.tr/		✓	Accept All / Reject All	X	Bottom Right	Clear
https://www.lcwaikiki.com/tr-TR/TR		✓	Manage Preferences/ Allow All Cookies/ Reject All Cookies	X	Website footer	Clear

4.4. France

French websites like 'amazon.fr,' 'carrefour.fr,' and 'fnac.com' were mostly GDPR-compliant as shown in Table 4, offering explicit consent options like "Configure," "Accept all," and "Manage my cookies." The use of pop-ups for these settings makes them more noticeable, and the language used is clear and straightforward, meeting GDPR is intelligibility requirements.

However, the presence of pre-ticked boxes in some instances indicates that even within the EU, where GDPR is law, compliance is not always fully realized. This represents a significant concern as it could be interpreted as a dark pattern, designed to manipulate user choices subtly.

Table 4. France Website Evaluation

Website	Implicit Consent	Explicit Consent	Consent Buttons	Presence of Pre-Ticked Choices	Banner Style	Use of Language
https://www.amazon.fr/gp/aw/c		✓	Accept/ Customize Cookies	X	Website footer	Clear
https://www.carrefour.fr/		✓	Configure/Accept all	X	Pop up	Clear
https://www.fnac.com/		✓	Manage my cookies/ Accept	X	Pop up	Clear
https://www.coursesu.com/drive/home		✓	Configure cookies/ Refuse All/Accept All	X	Website Footer	Clear
https://www.auchan.fr/		✓	Refuse/Accept/ Configure	X	Pop up	Clear
https://www.veepee.fr/gr/home/default		✓	Configure/ Allow all Cookies	X	Pop up	Clear
https://www.cdiscount.com/		✓	Configure cookies/ Accept	X	Pop up	Clear

4.5. United States

The US websites like 'rossstores.com,' 'michaels.com,' and 'amazon.com' offered varied approaches to cookie consent as illustrated in Table 5. While some like 'rossstores.com' used language such as "Accept Cookies/do not share my personal info," others simply stated, "I understand/do not share my personal info," which may not provide the clarity required under GDPR guidelines.

Table 5. United States Website Evaluation

Website	Implicit Consent	Explicit Consent	Consent Buttons	Presence of Pre-Ticked Choices	Banner Style	Use of Language
https://www.rossstores.com/		✓	Accept Cookies/do not share my personal info	✓	Website footer	Clear
https://www.michaels.com/		✓	Cookie Preferences/ Got it	✓	Bottom Right	Clear
https://www.burlington.com/		✓	Allow cookies/do not share my personal info	X	Website footer	Clear
https://www2.hm.com/en_us/index.html		✓	Accept all cookies/Cookie Settings	X	Bottom Right	Clear
https://www.zara.com/us/		✓	Configure cookies	✓	Bottom Right	Clear
https://www.ulta.com/		✓	I understand/do not share my personal info	✓	Pop up	Clear
https://www.amazon.com/		✓	Accept/ Customize Cookies	X	Website footer	Clear

Given that the United States does not have a federal equivalent of the GDPR, it is perhaps not surprising that some practices might not be fully compliant with European standards. Nevertheless, in a global digital marketplace, failure to adhere to international best practices may have repercussions, including for U.S. consumers increasingly concerned about data privacy.

The research highlights significant disparities in GDPR compliance and the use of dark patterns across countries. South African websites seem to employ implicit consent without giving users an explicit choice, a tactic that is far from GDPR-compliant and could be seen as a dark

pattern. European countries generally fare better, although there are still instances where compliance is incomplete, most notably with the use of pre-ticked choices. U.S. practices are varied, reflecting the lack of a single, comprehensive federal data protection law. These findings provide critical insights for consumers, policymakers, and businesses alike, stressing the need for a more harmonized, transparent, and user-centric approach to cookie consent globally.

5. CONCLUSION

Our study addresses a critical gap in existing research by providing a global, cross-continental analysis of dark patterns on e-commerce websites in the post-GDPR and CCPA era. This focus is particularly vital given the international nature of e-commerce and the ever-increasing need for data protection across borders. Our findings reveal inconsistencies in GDPR and CCPA compliance among e-commerce platforms worldwide, with many employing dark patterns that subvert the intended transparency and user agency these regulations aim to establish.

Our results indicate that while some progress has been made in aligning e-commerce practices with GDPR and CCPA guidelines, there remains significant room for improvement. Dark patterns continue to be a prevalent strategy to nudge consumers into actions that may not be in their best interest, despite existing legal frameworks designed to enhance online privacy and data protection.

Based on these findings, we recommend more stringent enforcement of GDPR and CCPA regulations, especially in the realm of e-commerce. Further, standardizing compliance requirements at an international level could provide clearer guidelines for multi-national e-commerce platforms. This would not only bolster consumer trust but also level the playing field for businesses striving to maintain both competitive advantage and regulatory compliance.

REFERENCES

Bongard-Blanchy, Kerstin, Arianna Rossi, Salvador Rivas, Sophie Doublet, Vincent Koenig, and Gabriele Lenzini. 2021a. " I Am Definitely Manipulated, Even When I Am Aware of It. It's Ridiculous!"-Dark Patterns from the End-User Perspective." In *Designing Interactive Systems Conference 2021*, 763–76.

Calzada, Igor. 2022. "Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)." *Smart Cities* 5 (3): 1129–50.

Economy, Elizabeth C. 2010. "The Game Changer-Coping with China's Foreign Policy Revolution." *Foreign Aff.* 89: 142.

Fokina, Maryia. 2023. "Online Shopping Statistics: Ecommerce Trends for 2023." 2023.

Geronimo, Linda Di, Larissa Braz, Enrico Fregnan, Fabio Palomba, and Alberto Bacchelli. 2020. "UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception." In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–14.

Goldman, Eric. 2020. "An Introduction to the California Consumer Privacy Act (Ccpa)." *Santa Clara Univ. Legal Studies Research Paper*.

Gray, Colin M, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L Toombs. 2018. "The Dark (Patterns) Side of UX Design." In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–14.

Habib, Hana, Megan Li, Ellie Young, and Lorrie Cranor. 2022. "'Okay, Whatever': An Evaluation of Cookie Consent Interfaces." In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, 1–27.

Kessler, Joanna. 2019. "Data Protection in the Wake of the GDPR: California's Solution for Protecting" The World's Most Valuable Resource"." *S. Cal. L. Rev.* 93: 99.

Kirkman, Daniel, Kami Vaniea, and Daniel W Woods. 2023. "DarkDialogs: Automated Detection of 10 Dark Patterns on Cookie Dialogs." In *8th IEEE European Symposium on Security and Privacy*. IEEE.

Ko, Haksoo, John Leitner, Eunsoo Kim, and Jonggu Jeong. 2017. "Structure and Enforcement of Data Privacy Law in South Korea." *International Data Privacy Law* 7 (2): 100–114.

Maier, Maximilian. 2019. "Dark Patterns–An End User Perspective." Dissertation

Mathur, Arunesh, Gunes Acar, Michael J Friedman, Eli Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan. 2019. "Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites." *Proceedings of the ACM on Human-Computer Interaction* 3 (CSCW): 1–32.

Mathur, Arunesh, Mihir Kshirsagar, and Jonathan Mayer. 2021. “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*, 1–18.

Nevala, Emma. 2020. “Dark Patterns and Their Use in E-Commerce.” Informaatioteknologian Tiedekunta

Nouwens, Midas, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. 2020a. “Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence.” In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–13.

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020, April). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In Proceedings of the 2020 CHI conference on human factors in computing systems (pp. 1-13).

Phillips, Mark. 2018. “International Data-Sharing Norms: From the OECD to the General Data Protection Regulation (GDPR).” *Human Genetics* 137: 575–82.

Rantos, Konstantinos, George Drosatos, Konstantinos Demertzis, Christos Ilioudis, Alexandros Papanikolaou, and Antonios Kritsas. 2019. “ADvoCATE: A Consent Management Platform for Personal Data Processing in the IoT Using Blockchain Technology.” In *Innovative Security Solutions for Information Technology and Communications: 11th International Conference, SecITC 2018, Bucharest, Romania, November 8–9, 2018, Revised Selected Papers 11*, 300–313. Springer.

Regulation, General Data Protection. 2018. “General Data Protection Regulation (GDPR).” *Intersoft Consulting, Accessed in October* 24 (1).

Rust, Roland T, P K Kannan, and Na Peng. 2002. “The Customer Economics of Internet Privacy.” *Journal of the Academy of Marketing Science* 30 (4): 455–64.

Santos, Cristiana, Midas Nouwens, Michael Toth, Nataliia Bielova, and Vincent Roca. 2021. “Consent Management Platforms under the GDPR: Processors and/or Controllers?” In *Annual Privacy Forum*, 47–69. Springer.

Shamsudhin, Naveen, and Fabrice Jotterand. 2022. “Social Robots and Dark Patterns: Where Does Persuasion End and Deception Begin?” In *Artificial Intelligence in Brain and Mental Health: Philosophical, Ethical & Policy Issues*, 89–110. Springer.

Soe, Than Htut, Oda Elise Nordberg, Frode Guribye, and Marija Slavkovik. 2020. “Circumvention by Design-Dark Patterns in Cookie Consent for Online News Outlets.” In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*, 1–12.

Spece Jr, Roy G, John K Hilton, and Jeffrey N Younggren. 2016. “(Implicit) Consent to Intimacy.” *Ind. L. Rev.* 50: 907.

"Statutes of the Republic of Korea." n.d. Accessed September 12, 2023. https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53044&lang=ENG.

Stöver, Alina, Nina Gerber, Christin Cornel, Mona Henz, Karola Marky, Verena Zimmermann, and Joachim Vogt. 2022. "Website Operators Are Not the Enemy Either-Analyzing Options for Creating Cookie Consent Notices without Dark Patterns." *Mensch Und Computer 2022-Workshopband*.

Toth, Michael, Nataliia Bielova, and Vincent Roca. 2022. "On Dark Patterns and Manipulation of Website Publishers by CMPs." In *PETS 2022-22nd Privacy Enhancing Technologies Symposium*.

Vijayan, Aiswarya. 2019. "Digital India-A Roadmap to Sustainability." *International Journal of Innovative Technology and Exploring Engineering* 8 (5): 571–76.

Wong, Richmond Y, Andrew Chong, and R Cooper Aspegren. 2023. "Privacy Legislation as Business Risks: How GDPR and CCPA Are Represented in Technology Companies' Investment Risk Disclosures." *Proceedings of the ACM on Human-Computer Interaction* 7 (CSCW1): 1–26.

Zaeem, Razieh Nokhbeh, and K Suzanne Barber. 2020. "The Effect of the GDPR on Privacy Policies: Recent Progress and Future Promise." *ACM Transactions on Management Information Systems (TMIS)* 12 (1): 1–20.