The University of Chicago Business Law Review

Volume 1
Number 1 *2022: Summer*

Article 19

6-1-2022

The FTC and the CPRA's Regulation of Dark Patterns in Cookie Consent Notices

Danyang Li
Danyang.Li@chicagounbound.edu

The FTC and the CPRA's Regulation of Dark Patterns in Cookie Consent Notices

Danyang Li[*]

Dark patterns are designed to confuse and manipulate users to select the option preferred by website owners. Dark patterns are especially prevalent in cookie consent notices, which are notices that websites display to inquire users regarding their cookie preferences. Cookies are often used by websites to track and store user information for functional and marketing purposes. Dark patterns exploit various psychological biases, and the interaction among the biases will likely exacerbate their effects. This Article examines 100 cookie consent notices from the most popular e-commerce websites in the United States and offers a set of empirical data on the current landscape of dark patterns in cookie consent notices. Based on our results and analysis, most cookie consent notices we examined are likely considered unfair and deceptive under Section 5 of the FTC Act. Moreover, under the CPRA legal framework, most notices are also considered coercive and manipulative. Future regulators should focus on the design of online consent mechanisms to better protect consumer interest in privacy.

I. INTRODUCTION 562
II. DARK PATTERNS 564
III. THE EMPIRICAL STUDY 570
A. Summary 570
B. Method 570
C. Results 572
IV. DISCUSSION AND ANALYSIS 574
A. The FTC Act 575
1. The Unfair Standard 575
2. The Deceptive Standard 579
3. The FTC's Enforcement Policy Statement on Negative Option Marketing 582
B. CCPA & CPRA 586
V. CONCLUSION 589

[*] J.D. Candidate 2023, The University of Chicago Law School

I. INTRODUCTION

As technology plays a larger role in society, it becomes much easier for internet companies to collect private information from their consumers. Nowadays, consumers often sign away their privacy rights without even reading the provisions. It has become instinctive for internet surfers to click on "consent to tracking" without even realizing what they are giving away. Consumers often face what is called a "privacy paradox," which refers to a gap between their desired state regarding privacy and their actual state.[1] Simply, there is a mismatch between consumers' expectation of privacy and their actual behavior of sharing their information.[2] People's beliefs in their privacy profile settings differ from their actual settings.[3] This further shows that consumers often have false impressions about how protected their private information is.

Moreover, website owners often manipulate their privacy settings to make it harder for consumers to protect their privacy. Recently, there have been efforts to create or update data privacy laws to target a phenomenon called dark patterns, which are user interfaces intentionally designed to confuse and manipulate users into taking certain actions that are not their actual preference.[4] Dark patterns exploit psychological biases and choice architecture to prompt users to make less deliberate and rational choices. Dark patterns are extremely prevalent. In an academic study, authors crawled more than 11,000 popular e-commerce websites and found dark patterns on 11% of them.[5]

However, no such study of dark patterns has been done on cookie consent notices, an area in which they are especially prevalent.[6] Cookies allow the websites to track user information for

---

1 Alessandro Acquisti et al., *Privacy and Human Behavior in the Age of Information*, 347 SCI. 509, 509–10 (Jan. 30, 2015).

2 *Id.*

3 Michelle Madejski et al., *A Study of Privacy Settings Errors in an Online Social Network*, *in* INST. OF ELEC. & ELECS. ENG'RS, 2012 IEEE INTERNATIONAL CONFERENCE ON PERVASIVE COMPUTING AND COMMUNICATIONS WORKSHOPS 340, 340–345 (2012).

4 *See* Jamie Luguri & Lior Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. LEGAL ANALYSIS 43, 48–51 (2021).

5 Midas Nouwens et al., *Dark Patterns After the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence*, PROC. 2020 CHI CONF. ON HUM. FACTORS COMPUTING SYS. 1–13 (2020).

6 *See* Christine Utz et al., *(Un)informed Consent: Studying GDPR Consent Notices in the Field*, CCS '19: PROC. 2019 ACM SIGSAC CONF. ON COMPUT & COMMC'NS SEC. 973, 973–90 (2019).

profiling and targeted advertising.[7] The cookie consent notices will typically ask for consent to data collection and state how the data will be used. [8] In this decision-making setting, users often have incomplete information regarding the cookie settings, which puts them at a disadvantage when compared with web designers.[9] This asymmetrical information will lead the users to fall prey to the many biases and dark patterns used by the web designer to nudge the users to accept all cookies. This Comment will introduce empirical data by analyzing the language and the user interface of the cookie consent notices across 100 popular e-commerce websites under the current legal framework regarding privacy in the United States.

There is currently no specific cookie law in the United States but data privacy law in general can regulate cookies. Data privacy law seeks to protect rights around the commercial use of personal private data, addresses the accessibility of personal data, and reduce the harmful impacts of data breaches.[10] Within data privacy law, the Federal Trade Commission (FTC), which is responsible for administering online privacy law, has recently enacted regulations against deceptive commercial practices under the Federal Trade Commission Act (FTC Act).[11] The FTC has the authority to regulate any use of unfair or deceptive practices affecting interstate commerce under Section 5 of the FTC Act.[12] In the cookie consent setting, many of the notices contain elements of unfairness and deception under this standard. The FTC has also recently issued an Enforcement Policy Statement which specifically listed the requirements for online disclosures, consent, and cancellation policy, all of which may be adopted to cookie consent notices.[13]

Moreover, at the state level, the California Consumer Privacy Act (CCPA) along with the California Privacy Rights Act (CPRA),

---

7 *See* Dominique Machuletz & Rainer Böhme, *Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs After GDPR*, 2 PROC. ON PRIVACY ENHANCING TECH. 481, 481–98 (2020).

8 *Id.*

9 *See* Alessandro Acquisti & Jens Grossklags, *What Can Behavioral Economics Teach Us About Privacy?*, *in* DIGITAL PRIVACY: THEORY, TECHNOLOGIES, AND PRACTICES 370 (Alessandro Acquisti et al. eds., 2008).

10 *See* Andraya Flor, *The Impact of* Schrems II*: Next Steps for U.S. Data Privacy Law*, 96 NOTRE DAME L. REV. 2035, 2039 (2021).

11 See Bradyn Fairclough, Privacy Piracy: *The Shortcomings of the United States' Data Privacy Regime and How to Fix It*, 42 J. CORP. L. 461, 467 (2016).

12 *Id.*

13 *See* Fed. Trade Comm'n, Enforcement Policy Statement Regarding Negative Option Marketing (Oct. 28, 2021).

which will fully replace the CCPA by 2023, aim to protect consumer privacy at the state level.[14] The CPRA has specific provisions targeting dark patterns and is set to regulate cookie consent notices. One scholar analyzed the definition of dark patterns under the CPRA but did not focus on cookie consent notices specifically.[15] But given that the CPRA specifically addresses dark patterns, it has the potential to regulate cookie consent notices.[16] Moreover, the CPRA also specifically prohibits coercive and manipulative consent, both of which are present in some of the cookie consent notices.[17] The CPRA will help provide a guideline on the future requirements of cookie consent notices.

This Comment will utilize empirical data collected from the cookie consent notices across 100 e-commerce websites to analyze those websites' compliance to the requirements of Section 5 of the FTC Act and the cookie consent requirements laid out by the CPRA.

II. DARK PATTERNS

Dark patterns are user interfaces designed to confuse and manipulate users into picking the choice preferred by the designers.[18] Dark patterns bar users from acting in accordance to their preferences. They are concerning because they undercut individual autonomy through deception and coercion.[19] They create false impressions that users have free choices while manipulating users into disclosing private information that they otherwise would not reveal.[20] Under the influence of biases and heuristics that dark patterns exploit, consumers are tempted away from making rational choices concerning their privacy.[21]

Dark patterns can induce users to make irrational choices because they prompt users to use System 1 decision-making, which relies on impulse and heuristics, instead of System 2, which

---

14 California Consumer Privacy Act, CAL. CODE REGS. tit. 11, § 999.315(h) (2021) [hereinafter CCPA]; *see also* Angelique Carson, *Data Privacy Laws: What You Need to Know in 2021*, OSANO (June 24, 2020), https://perma.cc/LZ23-269M.

15 *See* Jennifer King & Adriana Stephan, *Regulating Privacy Dark Patterns in Practice-Drawing Inspiration from California Privacy Rights Act*, 5 GEO. L. TECH. REV. 251, 259 (2021).

16 California Privacy Rights Act § 1789.140(1) (amended by 2021 Cal. Legis. Serv. Ch. 525 (A.B. 694) (West)) [hereinafter CPRA].

17 *Id.*

18 *See* Luguri & Strahilevitz, *supra* note 4, at 48.

19 *See* King & Stephan, *supra* note 15, at 259.

20 *See id.*

21 *See id.*

involves deliberate thinking.[22] Under System 1 decision-making, people will usually operate automatically and make quick judgments with almost no voluntary control.[23] System 2 allows people to allocate their attention to their complex and deliberate decision-making.[24] Dark patterns exploit System 1 decision-making and tempt users to make decisions quickly and unconsciously.

Figure 1

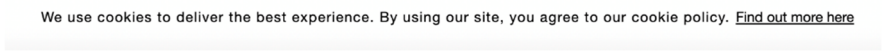
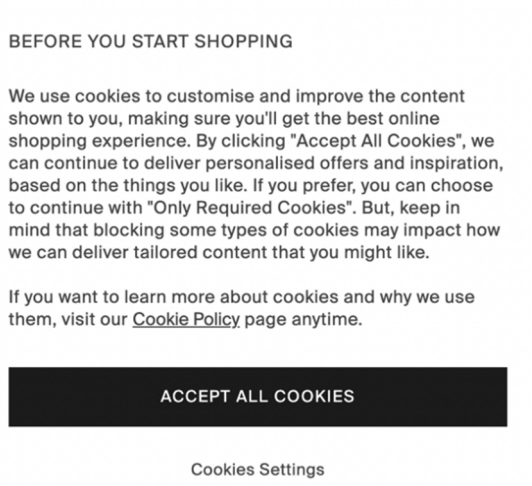


Figure 2



Regarding Cookie Notice Consent, many dark patterns are lurking not only in the structure and design of the notices, but also in the language of the notices. Luguri and Strahilevitz summarized existing dark pattern taxonomies. Many of the dark patterns mentioned are present in online cookie consent notices. Many cookie consent notices use "obstruction," which creates unnecessary barriers for users to reject cookies.[25] For example, in Figure 1, it is much easier to click "Accept All Cookies" then go to the cookie setting to deselect each non-necessary cookie. Another

---

22 *See* Daniel Kahneman, *Of 2 Minds: How Fast and Slow Thinking Shape Perception and Choice [Excerpt]*, SCI. AM. (June 15, 2012), https://perma.cc/DE6W-279K.

23 *See id.*

24 *See id.*

25 Luguri & Strahilevitz, *supra* note 4, at 53.

category of dark patterns used is "Interface Interference," which includes user interface manipulation like "confirmshaming" and "aesthetic manipulation."[26] Confirmshaming, for example, refers to when the cookie consent notice states that it will only deliver the best experience if a user accepts all cookies. The choice of rejecting all non-necessary cookies will be framed as "dishonorable" or "stupid."[27] Dark patterns like confirmshaming prompt the users to use System 1 decision-making instead of System 2 to deliberately make a decision. Aesthetic manipulation includes larger fonts and high contrast color on texts that the designers prefer the users to see, or at least see first, but minimizes or hides crucial information.[28] E-commerce websites also use the "Roach Motel" to make it very easy for a consumer to agree to certain terms but much harder for the consumer to get out of it.[29] For example, roach motel will manifest as a subscription service that makes it easy for consumers to sign up but makes it very difficult for them to cancel the subscription.[30] It is crucial to highlight the psychological biases internet companies and website designers use to collect user information and how to combat these dark patterns.

In one study, Luguri and Strahilevitz examined the effects of various dark patterns on users' decision-making processes.[31] The study asked participants to accept or decline a purchase for a data protection program. But the steps to do so involved different levels of dark pattern manipulation like preselecting the accept option or barriers to decline.[32] The researchers found that a binary choice of "Yes" or "Not Now" is "the most insidious" given that this kind of design can double the percentage of consumers who agree to accept some products preferred by the web designer.[33] The researchers also showed that obscuring information or confusing language makes customers profoundly more susceptible to accepting all terms without realizing what they are agreeing to.

Based on previous scholarship, consumers are very vulnerable to dark patterns because dark patterns are psychological manipulations designed to induce them to sign away their rights without realizing it, especially when it comes to privacy rights. This Comment will discuss several underlying biases that might

---

26 *Id.*
27 *Id.*
28 *Id.*
29 *Id.*
30 Luguri & Strahilevitz, *supra* note 4, at 53.
31 *See id.* at 61.
32 *Id.*
33 *Id.* at 81.

be at play when users are affected by the dark patterns in cookie consent notices: framing effects, defaults, Query Theory, nudges, cognitive dissonance, loss aversion, decision fatigue, and ambiguity aversion. These biases interact with each other to further reinforce the negative consequences of the dark patterns.

One of the underlying cognitive biases that might make consumers fall prey to data collection without recognizing it is a framing effect. A framing effect refers to the idea that one's decision might be affected by the way in which information is presented.[34] An internet company may frame the choice in a certain way that nudges the users to choose a setting that benefits the company. For instance, a website might present information that emphasizes the benefits of choosing to disclose personal data and downplays the risks associated with that choice. It might also manipulate the user's preference by varying color and font.

Saliency and ordering may interact with framing effects to enhance the nudging. People will be more drawn to salient information, which can manifest as larger font or high contrast color; and the order in which people process information will also change how people perceive it as the option first considered will invoke more associative memory, which is the ability to remember the relationship between different objects and items.[35] In the cookie consent context, people will likely first consider the "accept all cookies" option because it is more salient and triggers more associative memory surrounding it. This effect then will likely interact with the framing effect to induce the users to choose the option preferred by the web designer. Each of the cognitive biases listed above may be at play in terms of data collection. So, this Comment will examine how these different effects interact with each other to prevent users from being nudged towards a decision that might expose them to unnecessary risks.

Default options in cookie consent notice work especially well when there is no option presented (see Figure 2) and users will likely keep scrolling on the website without even recognizing the cookie consent notice. People are more likely to stay with the default setting.[36] Default options work since they present themselves as the recommended option and going along with defaults

---

[34] *See Framing Effect*, DECISION LAB, https://perma.cc/7KMW-WQLM (last visited Feb. 11, 2022).

[35] See Alessandro Acquisti et al., *Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online*, 50 ACM COMPUTING SURVS. 44:1, 44:18 (2017).

[36] *See id.* at 44:21.

often requires less effort.[37] This default effect may interact with Query Theory, which proposes that people's preferences can be moderated by available queries.[38] Query Theory refers to the idea that what people prefer depends on what they think of first.[39] In the cookie consent context, the extent to which people value privacy information will then depend on which option is first being considered. They will agree to accept all cookies if that is the default option.

Data privacy scholarship has recently focused on how subliminal hints, or "nudges," affect users.[40] Thaler and Sunstein defined a nudge as "any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives." [41] Nudges lead users to pick one option over another based on the designer's intention, since users are prompted to use System 1 decision-making and there is often asymmetric information available for users when it comes to privacy data decisions.[42] Asymmetrical information refers to the situation where one party has more access to information than the other party. This will cause differential valuation of the transaction and give the party with more information an advantage over the other party.[43] In this cookie consent context, the designers will successfully nudge the users to pick the option they prefer by making the option of accepting all cookies more salient and more readily available for users to click on.

More importantly, besides nudges and default effect, pre-decision cognitive dissonance might be at play during privacy setting decision-making. Cognitive dissonance refers to the idea that people prefer consistency and are motivated to act to reduce a state of dissonance after a decision that caused a discrepancy between their current state and their ideal state.[44] Pre-decision cognitive dissonance differs from the traditional notion of cognitive dissonance in timing as it happens before the decision-making.[45]

---

[37] *See* Eric J. Johnson & Daniel G. Goldstein, *Do Defaults Save Lives?*, 302 SCI. 1338, 1338–1339 (2003).

[38] *See* Idris Adjerid et al., *A Query-Theory Perspective of Privacy Decision Making*, 45 J. LEGAL STUD. S97, S97–S121 (2016).

[39] *See id.*

[40] Acquisti et al., *supra* note 35, at 44:25.

[41] Richard H. Thaler & Cass R. Sunstein, *Libertarian Paternalism*, 93 AM. ECON. REV. 175 (2003).

[42] *See* Acquisti et al., *supra* note 35, at 44:25.

[43] *See id.* at 44:4.

[44] *See* Leon Festinger, A Theory Of Cognitive Dissonance 25–60 (1957).

[45] S. Oshikawa, Cognitive Pre-Decision Conflict and Post-Decision Dissonance, 15 BEHAVIORAL SCI. 132, 132–140 (1970).

In the cookie consent context, it may be induced by the designers of the website prior to the users making a decision and the designers will then advocate a certain act like accepting the cookies to reduce that discrepancy by restoring the users' consonance.[46] In one study, researchers interviewed 14 participants about their privacy preferences regarding their location data and concluded that cognitive dissonance explained participants' irrational choices.[47] Cognitive dissonance will manifest in a cookie consent notice with language like "we only want to use cookies to ensure our website works, provides a great experience and makes sure that any ads you see from us are personalized to your interests. By using our site, you consent to cookies."[48] The user might feel uncomfortable not accepting all the cookies since they are afraid that otherwise the website will not function as well as it could, and the user will likely accept all of the cookies.

Cognitive dissonance is further reinforced by loss aversion and the fear of missing out. Loss aversion refers to the idea that people tend to be more averse to losses than the equivalent gains.[49] People are often loss averse due to the endowment effect, which describes the irrational tendency to value an owned object more than a similar, but unfamiliar one.[50] In the privacy context, when people feel that they are in control of their private information, they tend to resist losing it. But when they feel like they already lost it, they tend to value it less. Users are afraid of missing out on the best experience of what the website can provide and when they feel like they are already endowed with the website's best experience, they do not want to lose it.[51] This will create a discrepancy in the sense that they want the best experience without feeling like they are missing out. To seek consonance with their ideal state, they will be prompted to click accept all cookies. Moreover, due to the information asymmetry between the users and the designers, the users are unsure of what will happen if they choose to reject all cookies. This ambiguity and uncertainty

---

[46] See Paul J. Costanzo, *Revisiting Cognitive Dissonance Theory: Pre-Decisional Influences and the Relationship to the Consumer Decision-Making Model*, 2 ATL. MKTG. J., Apr. 2013, at 42.

[47] *See* Isha Ghosh & Vivek Singh, *Using Cognitive Dissonance Theory to Understand Privacy Behavior*, 54 PROC. ASS'N INFO. SCI. & TECH. 679, 679–680 (2017).

[48] IROBOT, https://perma.cc/36AV-A8MV (last visited Feb. 11, 2022).

[49] *See Loss Aversion*, DECISION LAB, https://perma.cc/KBC7-LRNV (last visited Feb. 11, 2022).

[50] *See Endowment Effect*, DECISION LAB, https://perma.cc/U99D-9SVG (last visited Feb. 11, 2022).

[51] *See* Acquisti et al., *supra* note 35, at 44:25.

will likely cause the user to pick the more certain choice. This phenomenon is known as the uncertainty aversion, where people tend to pick the known choice over the unknown.[52] When the current website with all cookies is presented as the certain choice, users will be induced to pick the certain option over the uncertain ones since they are unsure about what will happen after they reject all cookies. In the long term, these biases will interact with each other and cause users to repeatedly choose the option that the designers prefer rather than their actual preference.

Repeated actions will also become habitual due to decision fatigue. When users repeatedly encounter the same decision, they will rely more on heuristics and put less effort into decision-making since making a decision is mentally taxing.[53] Given that many websites now present the cookie setting notice, users often need to make repeated choices and one easily relies on System 1 to make a decision and choose the "Accept All Cookies" option preferred by the web designer.

III. THE EMPIRICAL STUDY

A. Summary

I conducted a field study of 100 cookie consent notices on top e-commerce websites to investigate the effects of different variables of the notices. These variables include blocking, number of choices available, purpose of the text, privacy policy link, and various formatting elements of the notices. Based on the results of the study, it appears that 80.9% of the cookie consent notices in Binary Options display dark patterns, including confirmshaming and ambiguous language.

B. Method

To investigate the effects of different properties of cookie consent notices, I conducted a field study of 100 cookie consent notices on top e-commerce websites, ranked by revenues and viewership in the United States.[54] Since not every website has a cookie consent notice, only the websites that have cookie consent notices

---

[52] *See Ambiguity (Uncertainty) Aversion*, BEHAVIORALECONOMICS.COM, https://perma.cc/6LNY-MSUB (last visited Feb. 11, 2022).

[53] *See* Shai Danziger et al., *Extraneous Factors in Judicial Decisions*, 108 PROC. NAT'L ACAD. SCIS. 6889, 6889–6892 (2011); Jonathan Levav et al., *The Effect of Ordering Decisions by Choice-Set Size on Consumer Search*, 39 J. CONSUMER RSCH. 585, 585–599 (2012).

[54] REVIEWSXP, https://perma.cc/7GEW-HDSJ (last visited Feb. 11, 2022).

are included in our study. This study adopts some of the same variables used in a prior study that systematically analyzed 1,000 cookie consent notices in popular European websites. These variables include blocking, number of choices available, and various formatting factors. They have been adapted to the United States.[55] Although the European study used a similar empirical data collection method and examined similar properties as this Comment, it did not analyze the data collected under the current United States regulatory framework. This field study includes seven parameters on the user interfaces of cookie consent notices, and I coded each parameter based on the criteria listed below:

(1) Blocking: a cookie consent notice is coded as blocking if it blocks a large part of the website so that without interacting with it, one cannot view the full website. Blocking includes two situations. (1) The website's content is blurred or dimmed, and the notice prevents the users from interacting with the website without interacting with the notice first. (2) The consent notice is too big (covers more than a quarter of the website) and prevents users from viewing the full website without first interacting with the notice.

(2) Number of Choices: the cookie consent notices are coded in three types based on how users will interact with the notices. (1) No-option: there is no option to interact with the notice, and the notice only informs the user, such as "This site uses cookies for analytics and to deliver Personalized content. By continuing to browse our site, you agree that you have read and understand our Privacy Policy."[56] (2) Confirmation-only: there is only one option for users to click on such as "OK" or "I agree," and clicking on that option is perceived as consent to all cookies. 3. Binary Option: there are two forms of binary option: one type displayed as "Accept All Cookies" and "Cookie settings," and the other displayed as either accept or reject cookies.

(3) Purpose of the Text: this parameter is coded based on the purpose of the text of the notice, either "general," which includes phrases like "to provide best experiences for users" or "specific," which mentions "advertisement use," or "marketing purposes."

(4) Privacy Policy: this parameter is coded based on whether there is a specific link to the privacy policy. The text has

---

55 *See* Utz et al., *supra* note 6, at 973–90.

56 APMEX, https://perma.cc/9Q7U-2Y4K (last visited Feb. 11, 2022).

to contain "privacy policy" and only a link of "cookie settings" is not coded as having a link to the privacy policy.

(5) Format of the Cookie Consent Notice: the format parameter is coded in three types: (1) Banners, which are usually at the bottom of the page and stay consistently visible. (2) Pop-ups, which are windows to the side that appear suddenly, and usually cover less than ¼ of the page. (3) Walls, which are windows that prevent users from interacting with the website until consent is given. When the format is coded as "Wall" it also entails blocking under the Blocking parameter.

(6) Nudging: a cookie consent notice is coded as nudging when there is aesthetic manipulation in the options to induce users to click on "Accept all cookies." Typical features include highlighted text, high contrast color, visually framed text, and dimmed advanced settings so that users have a harder time looking for them. Overall, nudging means that the web designer is making the "Accept All Cookies" option easier for users to click on. This is only relevant in the "Binary Option" category under the "Number of Choice" parameter since in the "No-option" and "Confirmation-only" category there is only one option or no option thus no need for aesthetic manipulation.

(7) The Text: this parameter is different from the previous six as it conducts qualitative analysis on the text of the notices and assesses whether if there is any dark pattern present in the language itself including confirmshaming, or obscure language that confuses users. This parameter will also analyze the frequency of words used and how the language affects consumers' online consent decisions. This parameter is more subjective in terms of coding.

C. Results

Our data set contains 100 cookie consent notices from the most popular e-commerce websites. Since there is currently no specific cookie consent law in the United States, many of the popular e-commerce websites do not contain any sort of cookie consent notices. Out of the top 50 most popular e-commerce websites, there are only 9 that have some sort of cookie consent notices. We gathered our data from popular e-commerce websites that contain cookie notices.

For (1) the Blocking parameter, 17% of the cookie consent notices are blocking the websites. For (2) the Number of Choices

parameter, 24% of the cookie consent notices are No-option, 29% of the notices are Confirmation-only, and 47% of the notices have Binary Options. For (3) the Purpose of the Text parameter, 62% of the cookie consent notices state general purpose and only 38% of the notices state specific uses like advertising purposes. For (4) the Privacy Policy parameter, 74% of the cookie consent notices have a privacy policy link. For (5) the Format parameter, 66% of the cookie consent notices are in the banner format, 23% of the notices are in the pop-up window format, and 11% of the notices are in the wall format. For the (6) Nudging parameter, 38% of the overall cookie consent notices contain nudging but out of the Binary Option category, 80.9% of the notices that contain binary options have nudging. Only 1% of the notices have opposite nudging, which means that the reject all cookies option is being highlighted instead of the accept all cookies option. (Parameter (1) through (6) are presented in Table 1).

For the (7) the Text parameter, 11% of the cookie consent notices contain language like "we use the cookies to give you the *best* experience." 3% of the notices mention giving users a "better experience." 21% of the notices contain the word "personalize" in phrases such as "to provide you with a personalized experience." 3% of the notices use the word "customize" in the same sense as the word "personalize." 18% of the notices use the word "enhance" in phrases like "to enhance user experience." 6% of the notices state that they use the cookies to "tailor" the content to users' interests. Only 3% of the notices mention that the user can withdraw their consent to the cookies. Only 2% of the notices mention that the user can reject the cookies. Only 7% of the notices mention the user can opt-out of the cookies. Only 5% of the notices mention that the user can disable the cookies. Only 2% of the notices mention that they will not use other cookies except the strictly necessary ones unless the user opts into them. 20% of the notices mention that the user can manage their cookie preferences. Only 5% of the notices that mention they store user information. Only 8% of the notices mention that the collection of data may be considered a "sale" under certain state laws to alert the users. Only 21% of the notices mention that they "collect" data through cookies (this includes phrases like "collection of data"). 33% of the notices mention "ads" or "ad" or "advertising."

17% of the notices mention using third-party cookies, 1% of the notices mention using first-party cookies, and 1% of the notices mention both. 27% of the notices refer to an unspecified party cookie, usually by using the phrase "We use cookies . . . ."

5% of the cookie consent notices mention California residents and 4% of the notices mention The California Consumer Privacy Act.

Table 1: Parameters of the graphical user interface of consent notices and their value across a sample of 100 cookie consent notices collected from the most popular websites in the United States

(1) Blocking		**(2) Number of Choices**		**(3) Purpose of the Text**	
Blocking	17%	No-option	24%	General Purpose	62%
No-Blocking	83%	Confirmation-only	29%	Specific Purpose	38%
		Binary Options	47%		
(4) Privacy Policy		**(5) Format**		**(6) Nudging**	
Has a privacy link	74%	Banner	66%	Nudging overall	38%
No privacy link	26%	Pop-up	23%	Nudging in Binary Options	80.9%
		Wall	11%	Opposite Nudging	1%

IV. DISCUSSION AND ANALYSIS

Based on the result of the empirical study, it appears that 80.9% of the cookie consent notices in Binary Options exhibit dark patterns, including confirmshaming and ambiguous language. This is harmful to users as they are giving out personal data without realizing it. More importantly, these dark patterns are very effective in misleading the users and inducing them to select the option that benefits the website. This section will first introduce the possible legal aspects of regulating cookie consent notices and then analyze the empirical results under the relevant legal framework. Section 5 of the FTC Act authorizes the FTC to regulate any unfair or deceptive trade practices that affect interstate

commerce, which arguably include cookie consent notices. The CCPA lists future requirements that specifically target dark patterns. Cookie consent notices that contain dark patterns can be regulated under both regulatory regimes. This Comment will discuss how the FTC and the California legal frameworks could be implemented to curtail the use of dark patterns in the cookie consent notices.

A. The FTC Act

The FTC Act gives the FTC authority over "any person, partnership or corporation engaged in or whose business affects commerce."[57] The FTC Act provides that "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."[58] Under Section 5 of the FTC Act, the FTC can regulate dark patterns as the Supreme Court has deferred to the FTC's interpretation of the Act in *FTC v. Sperry & Hutchinson Co.*[59] and held that the Commission is allowed to "proscribe practices as unfair or deceptive in their effect upon consumers."[60] Thus, the FTC under the scope of the Act has the authority to regulate any unfair or deceptive practices including dark patterns. This Comment is going to argue that cookie consent notices can be analyzed under both the "unfair" and the "deceptive" standard given they have the characteristics necessary to satisfy both standards.

1. The Unfair Standard

An act or practice is "unfair" if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[61] The "unfair" standard can be broken down into three elements with a focus on consumer harm:

> First, there must be a *substantial consumer injury*. This is an objective test. The Commission requires a real injury—emotional distress is not sufficient. The harm need not be large to any individual, but if it is significant in aggregate it may be substantial harm. The statement also notes that the harm

---

57 15 U.S.C. § 46(a).
58 15 U.S.C. § 45.
59 405 U.S. 233 (1972).
60 *Id.* at 239.
61 15 U.S.C. § 45(n).

> might be small as an absolute matter, but still substantial if it is significantly larger than the benefit. Second, the harm of the practice *must not be outweighed by countervailing benefits of that practice*. Finally, the harm *must not be reasonably avoidable by the consumer*. If the consumer could have avoided the harm by choosing differently, the FTC will respect the consumer's choice.[62]

Under Section 5 of the FTC Act, in a complaint against DSW, Inc., the FTC held that the company was engaging in an unfair practice when it "failed to provide reasonable and appropriate security for sensitive customer information" [63] and allowed hackers to access the credit card and checking account information for over 1.4 million customers.[64] DSW stored sensitive information in unencrypted files and failed to use available security measures to protect consumer information.[65] Furthermore, the FTC under Section 5 held that programs that download spyware onto users' computers without users' knowledge are unfair practices.[66] In a complaint regarding Seismic Entertainment Productions, the FTC found that it was an unfair practice to "compel" users to purchase a wiper program by compromising their computers in the first place.[67] The FTC also held that any operations that secretly download spyware was an unfair practice in itself.[68]

The "unfair" standard usually requires monetary harm to satisfy the "substantial injury" prong. However, the FTC notes that an injury may meet the substantiality standard if "it does a small harm to a large number of people."[69] One might argue that consumers who are induced to accept all cookies do not suffer substantial harm given that there is no monetary harm. But cookies have a wide range of uses including authenticating users and

---

62 Maureen K. Ohlhausen, *Weigh the Label, Not the Tractor: What Goes on the Scale in an FTC Unfairness Cost-Benefit Analysis?*, 83 GEO. WASH. L. REV. 1999, 2006 (2015) (citing FED. TRADE COMM'N., COMMISSION STATEMENT OF POLICY ON THE SCOPE OF THE CONSUMER UNFAIRNESS JURISDICTION (1980), *reprinted in Int'l Harvester Co.*, 104 F.T.C. 949, 1072–76 (1984)).

63 *DSW Inc. Settles FTC Charges*, FED. TRADE COMM'N. (Dec. 1, 2005), https://perma.cc/5GY3-XJJL.

64 Carolyn Hoang, *In the Middle: Creating a Middle Road Between U.S. and EU Data Protection Policies*, 32 J. NAT'L ASS'N ADMIN. L. JUDICIARY 810, 823 (2012).

65 *See DSW Inc. Settles FTC Charges*, *supra* note 63.

66 *See FTC Cracks Down on Spyware Operation*, FED. TRADE COMM'N. (Oct. 12, 2004), https://perma.cc/EV8W-F5V5.

67 *Id.*

68 *See id.*

69 *FTC Policy Statement on Unfairness*, FED. TRADE COMM'N (Dec. 17, 1980), https://perma.cc/E97V-CAQ6; *see* 15 U.S.C. § 45(n)).

securing their information. While some cookies only store website tracking information with unique identification numbers, other cookies will store consumer security information. It will vary on a case-by-case scenario, but a court may consider any kind of security breach or data leak as substantial harm, especially when users' information was being stored without their consent. If information is being sold to a third party without their consent, it might create identity theft risk if the information is not properly secured.[70] Identity theft is a cognizable injury that federal courts have long recognized.[71] Information sold to a third party without consent may itself constitute substantial harm, though this may be a weaker argument. Moreover, by profiling and tracking each consumer, some of the unnecessary cookies store and collect consumer information without clearly disclosing the usage of their data. 62% of the cookie consent notices state only the general purpose of their cookies. When combined with nudging, it is likely that most consumers will choose to accept all cookies without realizing what they are consenting to. Although this substantiality prong requires a "real injury" and not "emotional distress,"[72] there is still a possibility that this prong would be met as each consumer might suffer some small monetary damages by accepting the cookies. This small harm in aggregate creates substantial injury. This is a weaker argument as it might vary on a case-by-case approach, depending on whether there has been a data breach or whether consumers have suffered monetary damage from their data being sold to a third party without consent.

The next prong of the "unfair" standard addresses whether consumers could have reasonably avoided the injury. Practices that prevent consumers from making free market decisions will satisfy this prong.[73] In the cookie consent case, this prong is easily met as the dark patterns will hinder consumers from making their own effective decisions as 53% of the notices do not even present an option upfront (24% of the cookie consent notices are No-option, 29% of the notices are Confirmation-only), and out of the 47% of the notices that have Binary Options, 80.9% of the notices have nudging. The results of my empirical study present enough evidence to show that consumers are not making effective free decisions as they are often manipulated to accept all cookies.

---

70 *See DSW Inc. Settles FTC Charges*, *supra* note 63.

71 *See, e.g.*, United States v. Spears, 729 F.3d 753 (7th Cir. 2013).

72 Ohlhausen, *supra* note 62, at 2006.

73 Luguri & Strahilevitz, *supra* note 4, at 88.

The cost-benefit analysis prong of the unfairness standard recognizes that there might be benefits to certain practices. This prong is only satisfied when there are injurious effects that outweigh the benefits. In the cookie consent context, the benefits of protecting consumer privacy at large will likely outweigh any harm that may incur to the website owners for adjusting their privacy consent regimes. The cost-benefit analysis looks at the costs incurred for consumers as well as larger societal burdens and the cost for remedy. The FTC held in *FTC v. FrostWire, LLC* that a default preselection (roach motel) in a file-sharing app is both unfair and deceptive.[74] In this case, it is quite clear the harm outweighed the benefits because the consumer must go through an exceptionally difficult process to affirmatively unselect 190 files and prevent them from being shared while she only wanted to share ten of them.[75]

Regarding cookie notice consent, the inquiry should focus on whether the economic benefits of marketing and ads will outweigh the harm to consumers. Although marketing is an important tool for companies to gain sales, it should only be used when there is consumer consent and proper disclosure. Consumers' interests in privacy in the aggregate should outweigh the conveniences the companies receive for inducing consumers to accept all cookies given that it is much easier for companies to implement changes in their cookie notice regime. While marketing is important for the economy, it should not come at the expense of uninformed sales of consumer data. It is likely unreasonable to ban all cookies that collect consumer information, but it is reasonable to ban just the ones that improperly nudge consumers and are without clear disclosure. Companies should at least change their cookie notice regime to neutral notices without nudging and implement more disclosure-related education campaigns to increase consumers' awareness of privacy issues.

Overall, the "unfair" standard presents a potential source of authority to regulate cookie consent notices. The FTC can easily apply this test to cookie consent notices given the prevalent dark patterns present in most cookie consent notices. The only difficulty might be proving that the consumers suffered a real injury, which is based on whether the case contains a data breach or third-party involvement in illegal data sale.

---

[74] Complaint for Permanent Injunction and Other Equitable Relief, FTC v. Frostwire LLC, No. 11–CV–23643 (S.D. Fla. Oct. 12, 2011), 2011 WL 9282853.

[75] *Id.*

2. The Deceptive Standard

On the other hand, acts or practices are "deceptive" if there is "any 'representation, omission, or practice' that is (i) material, and (ii) likely to mislead consumers who are acting reasonably under the circumstances."[76] The first prong of materiality involves whether the information is going to affect consumer choice of a product, and any express claims regarding the product are presumptively material. [77] To impose liability under the second prong, the FTC does not need to prove that a majority of consumers believed a claim as false or misleading, as long as "at least a significant minority of reasonable consumers would be likely to take away the misleading claim."[78] There is also no need to prove intent.[79] If there is an "overall net impression" of the company's communication as false or misleading, the FTC can use its enforcement power.[80]

The FTC recently started to utilize its enforcement discretion to bring cases against businesses that made deceptive misrepresentations in their data privacy policy and hid unexpected data policies from consumers.[81] For example, the FTC asserted that Toysmart violated its own privacy policy when it shared consumer information in *FTC v. Toysmart.com, LLC*.[82] Similarly, the FTC asserted that the company also violated its own privacy policy by deceptively promising to not share consumer information in *Eli Lilly & Co.*[83]

More importantly, the Ninth Circuit regarded dark pattern techniques as deceptive practices in *FTC v. AMG Capital Management*.[84] The court held that to prevail under the deceptive practice standard, the Commission must establish a practice is likely to mislead reasonable consumers under similar circumstances.[85] This standard is supposed to be consumer-friendly and does not require actual proof of deception.[86] Instead, the FTC only

---

76 Luguri & Strahilevitz, *supra* note 4, at 83 (quoting *Cliffdale Assocs., Inc.*, 103 F.T.C. 110 (Mar. 23, 1984)).

77 *See* FTC v. Cyberspace.com LLC, 453 F.3d 1196, 1201 (9th Cir. 2006); *see also* FTC v. Pantron 1 Corp., 33 F.3d 1088 (9th Cir. 1994).

78 Fanning v. FTC, 821 F.3d 164, 170–171 (1st Cir. 2016).

79 *See* Luguri & Strahilevitz, *supra* note 4, at 83.

80 FTC v. E.M.A. Nationwide, Inc., 767 F.3d 611, 631 (6th Cir. 2014).

81 *See Fairclough*, *supra* note 11, at 467.

82 No. 00–11341, 2000 WL 34016434 (D. Mass. July 21, 2000).

83 133 F.T.C. 763 (2002).

84 910 F.3d 417, 424 (9th Cir. 2018), *rev'd and remanded on other grounds*, 141 S. Ct. 1341 (2021).

85 *Id.*

86 *Id.*

needs to show that there is a "net impression" that will likely mislead the consumers, even if the impression "also contains truthful disclosure."[87] The court focused on how a reasonable consumer under the circumstance would understand their obligation based on the terms of the debt agreement and determined that they likely could be misled by the representation there. Thus, the court held that the dark pattern technique in this case was deceptive.

The "deceptive" standard is the more applicable standard for cookie consent notices. The FTC has the authority to regulate the notices under this standard. The two requirements of the "deceptive" standard are materiality and the likelihood of misleading reasonable consumers.[88] The court held that the materiality requirement can be satisfied if the information present will likely affect consumer decision-making in *Cyberspace.com*.[89] For cookie consent notices, there are multiple features of the user interface of the notices that may present materiality concerns. First, 17% of the websites are using some sort of blocking to stop the users from accessing the web content before engaging with the notices. While there are benefits associated with a blocking feature as it will force readers to affirmatively choose some option, it likely is doing more harm than good since users are eager to assess the web content and with some nudging, they will be ready to click on accept all cookies. Second, for the Number of Choices parameter, 24% of the cookie consent notices present no option for users and 29% of the notices are Confirmation-only. These two types of notices present basically no choice for consumers and severely impair consumers' freedom to make a decision regarding their privacy. Third, for the Format parameter, the type of format will likely affect whether the consumer is going to engage with the website. 66% of the cookie consent notices are in the banner format, which makes it quite easy for consumers to view the website content without ever engaging with the notices. The other 34% of the notices (23% pop-up window format, and 11% wall format) will likely lead more consumers to engage with the notices.

Lastly, for the Nudging parameter, 38% of the overall cookie consent notices contain nudging, and 80.9% of the notices that contain binary options have nudging. The nudging will affect consumer choice by inducing them to pick the option preferred by the web owner. Moreover, the text of the notices itself is likely

---

87 *Id.* at 422 (quoting FTC v. Cyberspace.com LLC, 453 F.3d 1196, 1201 (9th Cir. 2006)).

88 Luguri & Strahilevitz, *supra* note 4, at 83.

89 *Cyberspace.com LLC*, 453 F.3d at 1201.

manipulative because only 7% of the notices mention the user can opt-out of the cookies and only 5% of the notices mention that the user can disable the cookies. Without disclosing that there are other options available, general notices will signal to users that they can only accept the cookies without other choices. For example, a cookie notice that does not have a privacy policy link and has a Confirmation-only feature could substantially influence consumer choice. The consumer might imply from the notice that they do not have other choices. Thus, the materiality prong is easily satisfied by these dark patterns presented in the notices.

The misleading prong is satisfied if the information's "overall net impression" is misleading.[90] In *AMG Capital Management*, the court held that information can be misleading even if it is "technically true."[91] The court then noted the various dark patterns used in the websites like default subscription and trick questions. In the context of cookie consent notices, the No-option and Confirmation-only format of the cookies will likely mislead reasonable consumers to think that they don't have other choices, especially when combined with general language like "we use the cookies to give you the best experience." Only 14% of the notices mention that users can reject, opt-out, or disable the cookies and only 20% of the notices mention that users can manage their cookie preferences. Users who are unfamiliar with the notion of cookies, which may be a majority of web users, do not know that they have the option to control their cookie settings with ambiguous and general language on the cookie consent notices.

Moreover, some of the ambiguous information included in the text will further mislead reasonable consumers. More than 30% of the notices contain the word "personalize," "customize," or "tailor" in phrases like "to provide you with a personalized experience." While these phrases are often utilized in marketing, in a cookie consent setting they are likely going to mislead users in the sense that they ambiguously state the purpose of the cookies without disclosing the fact that the cookies are actually storing and collecting user information for sale. Thus, it is likely that most of the current cookie consent notices will fall under the "deceptive" standard given that they contain information that will affect user decisions and mislead reasonable users. The regulation of cookie consent notices will be more suitable under the "deceptive standard" than under the "unfair" standard, though both

---

90 FTC v. E.M.A. Nationwide, Inc., 767 F.3d 611, 631 (6th Cir. 2014).

91 FTC v. AMG Cap. Mgmt., 910 F.3d 417, 424 (9th Cir. 2018), *rev'd and remanded on other grounds*, 141 S. Ct. 1341 (2021).

can apply to the cookie consent notices. The current cookie consent notices do not properly inform web users about their rights and the options they have to reject certain cookies. The majority of the cookie consent notices also are not obtaining "real" consent since most users do not pay attention to a consent notice banner that allows one to keep scrolling without engaging with the banner first.

3. The FTC's Enforcement Policy Statement on Negative Option Marketing

The FTC has recently started to address the problems regarding disclosure and consent. In a recent Enforcement Policy Statement,[92] the FTC provided specific guidance on how the existing law applies to negative option marketing, which manifests as "a term or condition under which the seller may interpret a consumer's silence or failure to take affirmative action to reject a good or service or to cancel the agreement as acceptance or continuing acceptance of the offer."[93] It would normally include features like "automatic renewals, continuity plans, free-to-pay or fee-to-pay conversions, and prenotification plans."[94] Consumers will suffer costs when there are inadequate disclosures and consumers are billed without their consent.[95] This is likely a version of roach motel where consumers have to jump through more hoops to get out of certain situations that they were induced easily to sign up for in the first place. The FTC is set to regulate these unfair or deceptive practices including hidden chargers, or seemingly "free" offers, or onerous cancellation and refund processes.

Under Section 5 of the FTC Act, the FTC has highlighted four basic requirements regarding negative option marketing. First, there must be clear and obvious disclosure regarding the material key terms of the offer including the existence of the negative option, the total cost, and the cancellation process. Second, the disclosure must happen before consumers agree to purchase the product. Third, the marketers must receive consumers' explicit informed consent. Lastly, the seller must not create unnecessary barriers to the cancellation or refund process to ensure the effectiveness of the process and must honor the cancellation terms.[96]

---

92 *See* FED. TRADE COMM'N, *supra* note 13.
93 *Id.* at 1.
94 *Id.*
95 *See id.* at 2.
96 *See id.* at 4–5.

In the Statement, the FTC also cited the Restore Online Shoppers' Confidence Act (ROSCA)[97] to address the current problems with online negative option marketing. ROSCA protects consumers from being charged for goods or services sold online through negative option marketing unless the seller: "(1) clearly and conspicuously discloses all material terms of the transaction before obtaining the consumer's billing information; (2) obtains a consumer's express informed consent before charging the consumer's account; and (3) provides simple mechanisms for the consumer to stop recurring charges."[98]

The FTC also promulgated the "Use of Prenotification Negative Option Plans" Rule (Prenotification Plan Rule), which requires the sellers to disclose several material terms. These include minimum purchase obligations, right to cancel, timeline to reject a selection, the return process, and the frequency with which announcements and forms will be sent.[99] This rule is enacted specifically to address the barriers to unsubscribing, and all the dark patterns related to subscription services.

Overall, the Policy Statement lists the requirements for disclosure, consent, and cancellation regarding negative option market. Although the Statement does not mention web cookie consent specifically, this Statement will help us establish a guideline for future regulations regarding cookie consent. The Statement requires a "clear and conspicuous" disclosure, and these disclosures should be "easily understandable by ordinary consumers."[100] The Statement also makes clear that the "marketers should obtain the consumer's express informed consent before charging the consumer."[101] The Statement further stresses that the cancellation process should be "simple" and "reasonable for consumers."[102]

There are two regulatory frameworks that can be extended to regulate the cookie consent notices: ROSCA and Prenotification Plan Rule. Under the FTC Section 5 and ROSCA, most of the cookie consent notices are likely not compliant with the requirements listed by the FTC. ROSCA regulates the disclosures, consent, and cancellation of negative option marketing. In the context of cookie consent, the first two areas of disclosures and consent can be directly applied to cookie consent notices; the

---

97 15 U.S.C. §§ 8401–8405.
98 *Id.*
99 16 C.F.R. Part 425.
100 FED. TRADE COMM'N, *supra* note 13, at 11.
101 *Id.* at 13.
102 *Id.* at 14.

cancellation policy may provide guidance for the rejection of cookie usage.

Applying the principle of disclosures under ROSCA to cookie consent notices will require clear and conspicuous disclosures from the website owners. This principle, if applied to the cookie consent notices, requires that at minimum that any material terms should be "difficult to miss (i.e., easily noticeable) or unavoidable and easily understandable by ordinary consumers."[103] The visual interface of the cookie consent notice should by "its size, contrast, location, the length of time it appears, and other characteristics" stand out from its background to be easily understood. Under this standard, the notice interface will be scrutinized for its appearance and its location on the screen. Potentially, any cookie consent notices that are too small, or do not stand out in a high contrast fashion will be deemed unlawful. Moreover, any cookie consent notices that do not appear for an extended period will be deemed problematic. This Statement also requires that any disclosures be "unavoidable."[104] Cookie consent notices under this requirement should disallow consumers to bypass the notices without interacting with them. The Statement also specifies that disclosure will fail the clear and conspicuous requirement if "a consumer needs to take any action, such as clicking on a hyperlink or hovering over an icon, to see it." Privacy links hidden behind a hyperlink might be considered a problem under this example, especially when the cookie consent notice is in the No-Option format.

Moreover, the Statement includes language that can be interpreted to prohibit dark patterns. The Statement specifies that a clear disclosure should not include "any information that interferes with, detracts from, contradicts, or otherwise undermines the ability of consumers to read and understand the disclosures."[105] Dark patterns often manipulate how the information is presented to distract consumers from the material terms that they should pay attention to including nudging or confirmshaming. This specific clause will help the FTC to regulate dark patterns that undermine consumers' ability to under the disclosures.

In terms of consent, ROSCA requires "consumers' express informed consent," and this requirement applied to cookie consent notices will oblige website owners to inform the consumers and

---

103 *Id.* at 11.
104 *Id.*
105 *Id.* at 12.

obtain their express consent.[106] Additionally, the website owners should have the ability to verify the consent.[107] This consent provision will help the FTC to provide more guidelines when it comes to obtaining consent from consumers.

The cancellation policy, while not directly applicable, can provide helpful guidance on what the rejection process should look like in the cookie consent context. ROSCA requires the cancellation process to be as easy as the initiation process, and through the same medium.[108] The cancellation process should be effective and simple, and the website owner should not obstruct this process.[109] If ROSCA applies, the owner should satisfy both the statute and Section 5 of the FTC Act.[110] In the cookie consent notice context, the rejection process should be just as easy and simple as the cancellation process outlined in ROSCA. The rejection should be accessible and through the same medium, which means neither the No-Option nor Confirmation-Only format should be allowed under this guideline. Even when it comes to Binary-Option format, the rejection button should be in the same format as the consenting button. Nudging the users to click on the consenting button or creating barriers for rejection will likely be unlawful if the FTC chooses to follow the same guideline for cookie consent notices.

The Prenotification Plan Rule is also helpful in providing a guideline for future cookie regulations even though it does not directly apply to cookie consent notices. The Prenotification Plan Rule targets plans that abuse a consumer's nonaction and take nonaction as consent to keep subscribing or purchasing. Although this Rule might have limited coverage as it only applies to negative option marketing, it can be interpreted as the FTC's effort to strike down the manipulative tactic of taking nonaction as consent. Applying it to the cookie consent context will allow the FTC to regulate any cookie consent notices that allow nonaction as a form of consent including the No-Option format notices. This Rule will require the website owners to obtain express consent from consumers.

Under this new Policy Statement, we can clearly see a trend in how the FTC is exercising its authority to restrict more dark patterns in commercial activities online. The FTC is providing

---

106 *Id.* at 13.
107 *See id.* at 14.
108 *See id.*
109 *See id.*
110 *See id.* at 15.

more specific guidelines for disclosures, consent, and the rejection process, all of which can be applied to the regulation of cookie consent notices. The FTC should adopt the content of this Policy Statement and use its authority to regulate cookie consent notices.

B. CCPA & CPRA

The CCPA applies when a business "does any amount of business in California and has more than $25 million in revenue, received or shares personal information for commercial purposes of 50,000 or more consumers, or derives fifty percent or more of its annual revenue from selling consumers' personal information."[111] The CCPA also covers businesses that exist entirely outside California.[112] The CCPA listed four major rights: "[t]he right to know about the personal information a business collects about them and how it is used and shared. The right to delete personal information collected from them (with some exceptions). The right to opt-out of the sale of their personal information. The right to non-discrimination for exercising their CCPA rights."[113]

The CCPA was modified in March of 2021 to "address attempts to subvert or impair Californians' ability to opt-out of sales of their personal information."[114]Although the CCPA did not use the term "dark patterns," it established a baseline condition for what to avoid: "[a] business's methods for submitting requests to opt-out shall be easy for consumers to execute and shall require minimal steps to allow the consumer to opt-out. A business shall not use a method that is designed with the purpose or has the substantial effect of subverting or impairing a consumer's choice to opt-out."[115]

The CPRA will replace the CCPA in 2023 and specifically addresses dark patterns.[116] It defines a dark pattern as: "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."[117] Moreover, the CPRA

---

111 Kiran K. Jeevanjee, *Nice Thought, Poor Execution: Why the Dormant Commerce Clause Precludes California's CCPA from Setting National Privacy Law*, 70 AM. U. L. REV. F. 75 (2020).

112 *Id.* at 89.

113 CCPA, *supra* note 14.

114 *Id.*; King & Stephan, *supra* note 15, at 254.

115 CCPA, *supra* note 14.

116 CPRA, *supra* note 16.

117 *Id.*

expressly stated that, "Likewise, agreement obtained through use of dark patterns does not constitute consent."

Regarding obtaining consent, the CPRA addressed two situations where consent may still be invalid, even though a dark pattern is not unfair or deceptive: there cannot be coercive consent or manipulative consent.[118]

Coercive consent happens when people think they are constrained by their options and the only rational option "is the one that the coercer intends."[119] Under the coercive influence, the individual is still able to make a choice, "just perhaps not the one they might have arrived at of their own accord . . . ."[120] Coercive consent also utilizes many of the psychological biases in dark patterns. For example, by limiting the option to Confirmation-only, the cookie consent notices are using default effect and nudging. In practice, this [practice?] will manifest as "control by the designer over the range of possible decisions, or the 'decision space.'"[121] Limiting this space will allow the designer to control the number of options available to users and nudge them to pick an option that the designer wants.[122] Having a Confirmation-Only option also signals to the users that there is no other option available. This option is often represented as a cookie consent notice with the "Accept All Cookies" button highlighted and with larger font, while the other non-consenting option "cookie setting" is in a smaller, less obvious color.[123] Web designers may present a consent notice without putting a link for their privacy policy on the front page to make consumers less aware of their rights.[124] Based on our study, 26% of the cookie consent notices do not have a privacy policy link.

The CPRA requires that the website allow consumers to "revoke the consent as easily as it is affirmatively provided."[125] This is similar to the provision of the Prenotification Plan Rule by the FTC as it also requires that consumers should not face more barriers when it comes to opting out of services that they easily

---

118 *Id.*

119 Daniel Susser et al., *Technology, Autonomy, and Manipulation*, 8 INTERNET POL'Y REV. 1, 4 (2019).

120 King & Stephan, *supra* note 15, at 269.

121 *Id.* (quoting Arunesh Mathur et al., *What Makes a Dark Pattern . . . Dark?: Design Attributes, Normative Considerations, and Measurement Methods*, PROC. 2021 CHI CONF. ON HUM. FACTORS COMPUTING SYS. (2021)).

122 *Id.*

123 *See supra* Figure 1.

124 *Id.*

125 CPRA, *supra* note 16, at § 1798.135(b)(2)(A).

signed up for before. This CPRA standard will create a baseline requirement that the rejection process should not be burdensome for consumers.[126] Applying this standard to cookie consent notices will likely mean that all cookie notices should at least have a "Reject" button alongside the "Accept" button to make it compatible in terms of effort in accepting or rejecting the cookies. The current Confirmation-only format is not allowed under this standard since the opting-out and rejecting process for cookie consent is much more difficult than the opting-in process. This resulted in barriers for consumers to reject cookies and is likely considered illegal under the CPRA regulatory regime. Companies should at least create neutral user interfaces to make the process of rejecting cookies just as easy as that of accepting cookies.

Manipulative consent is different from coercion and deception in that it is often "hidden influence—the covert subversion of another person's decision-making power."[127] This means that the choice has already been made for the user without the user taking direct action. In practice, manipulative consent may manifest as a cookie consent notice that states, "By using our site, you agree to our cookie policy." (See Figure 2). Manipulative consent also utilizes similar psychological biases in dark patterns and induces users to pick the option preferred by the web designer. The CPRA includes specific language addressing manipulative consent: "[a]cceptance of a general or broad terms of use or similar document that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent."[128] Applying this language to the context of cookie consent banners will likely ban any No-option format that allows users to engage with the website content without interacting with the cookie consent notice. Often No-option cookie consent notices are not effective in alerting the users of their rights in privacy and the current regulation is not properly protecting users from privacy invasion.

Moreover, clicking "I Agree" on a cookie consent notice often represents multiple layers of consent with a single interaction, which can be problematic under the CPRA.[129] Often, the cookie consent notice will state that by clicking "I Agree" the consumers consent to the cookie usage policy and the privacy policy as well.

---

126 King & Stephan, *supra* note 15, at 270.

127 Susser et al., *supra* note 119, at 3.

128 CPRA, *supra* note 16, at § 1798.140(h).

129 King & Stephan, *supra* note 15, at 271.

The website is asking the consumers to consent to two different policies through one single interaction and they cannot do so separately. If consumers do not have the meaningful ability to make a decision regarding their privacy decisions but are instead forced to face all decisions at one single interaction, this might lead to the question of whether this consent is obtained through manipulative means.[130]

Both manipulative and coercive consent are deemed problematic under the CPRA and the majority of cookie consent notices obtaining consent in a manipulative and coercive manner would likely be considered unlawful. This will have a profound impact on how we think about consent and privacy if the CPRA is adopted as it is right now and it will help protect consumer interest in privacy.

V. CONCLUSION

The proliferation of dark patterns online raises important legal and ethical issues in our society today. Dark patterns not only pervade our personal private space online and cause us substantial financial harm,[131] but they also infiltrate our lives in a way that will alter how we behave in the long term. Understanding how dark patterns work psychologically is the first step to prevent them from being exploited by firms to harm consumers. This Comment addresses only a small area where dark patterns invade our lives in the online consent scenario. Combined with new technology, dark patterns raise novel legal issues for legal scholars and regulators. Federal and state regulators have now an opportunity to profoundly change the legal landscape of the online consent regulatory regime, and there is clearly a need to reevaluate the enforcement law regarding the online consent mechanism.

With increased attention on regulating dark patterns, both the FTC and the CPRA have the potential legal authority to provide specific regulations of dark patterns in cookie consent notices. Under Section 5 of the FTC Act, the FTC can regulate dark patterns in cookie consent notices under both the unfairness and deceptiveness standard. Courts have been generally receptive to these causes in a few FTC deception and unfairness cases. The FTC has also issued a new Enforcement Policy Statement on Negative Market Option to provide specific guidelines on disclosure, consent, and cancellation policy, all of which may be adopted to

---

130 *Id.*

131 *See DSW Inc. Settles FTC Charges*, *supra* note 63.

regulate dark patterns in cookie consent notices. Moreover, the CPRA specifically addressed dark patterns, and explicitly prohibited coercive and manipulative consent. Both the FTC Act and the CPRA provide guidance on how to regulate dark patterns in the future.

This Comment contributes to the existing literature by providing a new set of empirical data regarding dark patterns and specifically on cookie consent notices. The empirical study provides insights on the current state of cookie consent notices, which demonstrates the proliferation of dark patterns in the notices. Furthermore, this Comment also explains how various underlying psychological biases affect consumers when they encounter dark patterns online. The interaction among different biases will further exacerbate the effects of dark patterns, and facing online consent choices on a daily basis will likely create decision fatigue and change how people think about their privacy in the long term. Under both the FTC and the CPRA legal framework, most of the cookie consent notices analyzed under our study exhibit potentially unlawful usage of dark patterns.

In thinking about privacy issues, regulators can now target the problem from a new perspective by reconsidering the fundamental design of online consent mechanisms from both legal and psychological aspects. The possibility of future regulations for dark patterns and privacy in general will likely depend on social and empirical studies that assess consumer behaviors in the aggregate. These regulations will move towards a human-centered approach to better protect consumer privacy online.