Forthcoming Litigation for Companies That Employ Dark Patterns

Rachel Finegold*

I. INTRODUCTION

When you enter a company's website, perhaps to buy a product, it is common to receive a pop-up message that asks you to enter your email address to receive promotional materials. The options presented to you in this pop-up may read something akin to "I like to stay informed," and "I like to be left out." However, if the website is attempting to make you feel bad about declining to provide your personal information, then you may have experienced a dark pattern. Dark patterns are "digital design techniques that may manipulate consumers into buying products or services or giving up their privacy."[1] As a result, dark patterns inhibit consumer autonomy by steering them "to take actions they would not otherwise have taken."[2] For instance, if a company makes it harder to cancel a service than it was to sign-up for it, then the business is likely employing a dark pattern.[3] In doing this, the business hopes to subtly cause a consumer to become frustrated or confused with the cancellation process and avoid following through with their true intention. The business' goal is to skew the effort a user must exert when attempting to make a decision that would either reduce the company's profits or the amount of personal information it is collecting about a user, or both.[4]

This article will follow the emergence of dark patterns as the term legally crystallized. First, it will outline the path of the Federal Trade

* University of Chicago Law School '26.

[1] Press Release, F.T.C., FTC, ICPEN, GPEN Announce Results of Review of Use of Dark Patterns Affecting Subscription Services, Privacy (July 10, 2024), https://perma.cc/4XK7-MKSZ [hereinafter FTC Announces Dark Pattern Results].

[2] *Id.*

[3] OECD, *Dark Commercial Patterns*, OECD DIGITAL ECONOMY PAPERS 1, 8-9 (Oct. 26, 2022), https://doi.org/10.1787/44f5e846-en.

[4] *Id.*

Commission's ("FTC" or "Commission") enforcement of dark patterns. The agency's allegations begin with the more straightforward case of a company that illegally collects users' personal information *without providing any opportunity* to opt-out. Then, as the Commission begins establishing its basis to explicitly allege that a company has employed dark patterns directly in the complaint itself, the agency is able to target the more complicated dark pattern schemes we commonly see today. This includes when a company *deceives a consumer into unknowingly* allowing the collection of their personal information when it was never the consumer's true intention to do so. Next, the FTC's path is compared to the state of California, which is also developing its ability to litigate against companies that employ dark patterns. Finally, as both the FTC's and California's paths share many similarities, this article will conclude with how California's increased attention toward dark patterns will continue to progress; companies who employ dark patterns should expect enforcement action to be taken against them. Overall, this article will highlight the impact of including the term dark pattern as an allegation in the plaintiff's complaint, defining the term and its parameters within the law, and the particular importance for California businesses to avoid employing dark patterns.

II. ANALYSIS

A. The Materialization of Dark Patterns

The FTC, as part of its mission to stop deceptive or unfair business practices in the marketplace, has been taking action against companies who engage in these misleading and manipulative behaviors, predominantly under the agency's section five authority.[5] As a result, the FTC brought enforcement actions against companies who used similar behaviors to those captured by the term dark pattern even before the word was coined in 2010.[6] The FTC's first public settlement regarding internet privacy was in 1999.[7] In *In re GeoCities*, users were required to complete a new member application to use the website's services.[8] The form required personal information about the user, but the company, GeoCities, falsely conveyed the business' purpose for needing this

[5] Federal Trade Commission Act, 15 U.S.C. § 45(a)(1) (2018).

[6] *Bringing Dark Patterns to Light*, F.T.C. 1 (Sept. 2022), https://perma.cc/T8E5-PVM4; *see* Maydeen Merino, *FTC's War on 'Dark Patterns' Derives From Years Opposing Deceptive Practices, Ex-Agency Leaders Say*, NAT'L L. J. (June 20, 2024), https://perma.cc/34KT-AAYB (pointing out that even before the FTC called these behaviors dark patterns, the agency was spending "a lot of time going after companies that were making it easy to sign up and very difficult to quit").

[7] Press Release, F.T.C., Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case (Aug. 13, 1998), https://perma.cc/T8E5-PVM4.

[8] Complaint at ¶ 7, *In re Geocities* (F.T.C. 1999) (No. C-3850), https://perma.cc/G8FB-55T9 [hereinafter *In re Geocities* Complaint].

personal information.[9] While GeoCities stated it would only use personal information to gain a better understanding of its member base and help the company address member requests, GeoCities was actually sharing users' personal information with advertisers.[10] Hence, the FTC's action targeted a company who falsely stated what it was doing with members' personal information, and in doing so, misled consumers. Without the crystallization of the term dark pattern, the agency was relatively constrained to bringing suits against a company's more blatantly deceptive practices[11] without extending to the more nuanced deception associated with dark patterns today.[12]

In 2010, the same year the term dark pattern was coined, Congress enacted the Restore Online Shoppers' Confidence Act ("ROSCA"),[13] which gave the FTC more authority to try cases where companies took action without consumers' consent.[14] Where the FTC's section five authority falls short, ROSCA is able to fill in a few of the gaps.[15] The mission of ROSCA is to prohibit sellers from charging consumers via internet transactions without having clearly disclosed all material terms of the transaction and having obtained the consumers' express informed consent.[16] In 2014, the FTC successfully brought a case, under both ROSCA and the FTC's section five authority, against three technology companies who failed to clearly disclose that consumers would incur automatic monthly charges for using the defendants' services.[17] The basis for the FTC's argument is that the companies' act of interpreting "the consumer's silence or failure to take an affirmative action" as an "acceptance of the offer" violated section four of ROSCA.[18] At this time, the FTC also saw increased success in similar cases where a company blatantly lies to consumers, hides pertinent information, or disregards consumer directives.[19]

---

[9] *Id.* at ¶¶ 7, 12-14.

[10] *Id. at* ¶¶ 12-14.

[11] *See* Complaint at ¶¶ 13-16, *In re Gateway Learning Corp.* (F.T.C. 2004) (No. C-4120), https://perma.cc/DM6N-YPMB (alleging the defendant corporation's initial policy stated it would not share or sell users' personal information with third parties, and if the company materially changed its policy, it would then notify consumers. However, the company had sold its users' personal information to third parties and retroactively applied a revised policy stating the company would do so from time to time, but did not notify users of this policy change).

[12] *See* Complaint at ¶¶ 1-3, *FTC v. Publishers Clearing House LLC* (E.D.N.Y June 26, 2023) (No. 23-cv-4735), https://perma.cc/B6JD-AE36 (alleging defendant uses dark patterns) [hereinafter *Publishers* Complaint].

[13] Restore Online Shoppers' Confidence Act, 15 U.S.C. §§ 8401-05 (2010).

[14] *See* Merino, *supra* note 6.

[15] Becky Chao, Eric, Null & Claire Park, *The FTC is Currently the Primary Privacy Enforcer but its Authority is Limited*, NEW AMERICA (Nov. 20, 2019), https://perma.cc/D3LN-DR9P.

[16] 15 U.S.C. § 8402.

[17] Complaint at ¶¶ 24-34, 58, *FTC, State of Ill., State of Ohio v. One Tech., LP, One Tech. Mgmt., LLC, One Tech. Cap., LLP* (N.D. Cal. Nov. 2014) (No. 3:14-cv-05066), https://perma.cc/775C-GTEG (stipulating an order for permanent injunction and monetary judgment).

[18] *Id.* at ¶ 48; 15 U.S.C. § 8403.

[19] *See, e.g.*, Complaint, *In re Upromise, Inc.* (F.T.C. 2012) (No. C-4351), https://perma.cc/T3DE-39XL (alleging that despite the defendant's statement that its collection of consumer browsing information would remove personal identifiers, the company actually collected sensitive information such as credit card numbers and Social Security numbers); Complaint, *In re Chitika, Inc.* (F.T.C. 2011) (No. C-4324),

Yet, the FTC still faced challenges when consumers were deceived into checking a box that allowed the company to collect and share consumers' personal information such that their autonomy was reduced, and consent was in fact not obtained. For instance, in 2015, the FTC brought a suit against DirecTV alleging the defendant's website hid material details of the agreement from consumers because some information only became visible after the user hovered over a small 'Additional Offer Details' button at the bottom of the page.[20] The FTC argued DirecTV violated ROSCA by not clearly obtaining consumers' express, informed consent, since the deceptive design of the webpage did not show all material terms of the transaction.[21] However, due to the court's skepticism that the FTC would be able to prove consumers were misled by this design, the FTC agreed to voluntarily dismiss this claim with prejudice in 2018.[22] This same year, a commissioner of the FTC announced an agenda to identify "any additional tools or authorities the Commission may need to adequately deter unfair and deceptive conduct related to privacy."[23] As such, there is a "possibility that the FTC can further maximize its enforcement reach . . . through strategic use of additional remedies."[24] Hence, it is evident the agency still faced challenges in successfully bringing actions against companies who employ manipulative and deceptive practices that reduce consumer autonomy in more nuanced ways than the cases the FTC has typically been able to settle up to this point.

As dark patterns continued to grow exponentially in scale and sophistication, the FTC released a report in 2022 on some of the different ways coercive behaviors may violate the law in an attempt to keep pace with the evolving practices used in the marketplace.[25] In releasing this report, which was intended to "send a clear message that these traps will not be tolerated," the FTC was effectively alerting companies to the fact that dark patterns are not only a priority for the agency, but that it would be taking prompt action against those who employ them.[26] Subsequently, the FTC did just this and brought a barrage of cases charging defendants for using design tricks to avoid obtaining express consent. The FTC brought a case against Epic Games

---

https://perma.cc/8HEG-LDRN (describing how users who completed the opt-out process offered by defendant would only have their preferences honored for ten days before expiring).

[20] Complaint at ¶¶ 20-24, *F.T.C. v. DirecTV, LLC* (N.D. Cal. 2015) (No. 3:15-cv-01129), https://perma.cc/2XUU-UVK5.

[21] *Id.*

[22] Dorothy Atkins, *FTC Drops $4B False Ad Suit Against DirectTV Midtrial*, LAW360 (Oct. 2018), https://perma.cc/348H-QG2J.

[23] Hearings on Competition and Consumer Protection in the 21st Century, 83 Fed. Reg. 38307, 38309 (Aug. 6, 2018).

[24] Public Statement, F.T.C., Concurring Statement of Chairman Joe Simons, *In re Sandpiper/PiperGear and Patriot Puck* (Apr. 17, 2019), https://perma.cc/L8LH-QJTN.

[25] Press Release, F.T.C., FTC Report Shows Rise in Sophisticated Dark Patterns Designed to Trick and Trap Consumers (Sept. 15, 2022), https://perma.cc/R8GJ-PJZZ.

[26] *Id.*

alleging the company uses "dark patterns" to deter users from cancelling or requesting refunds for unauthorized and unintentional in-game purchases.[27] Epic Games settled for $245 million.[28] The FTC also sued Publishers Clearing House for using "dark patterns" to "deceive consumers into believing they must order products before they can enter the sweepstakes" by, among other things, using "tricky wording," and "placing disclosures in small and light font in places where a consumer is unlikely to see them."[29] Publishers Clearing House settled for $18.5 million.[30] Additionally, the FTC targeted the company Doxo for deploying an array of "dark patterns" through deceptive design tricks, such as when the defendant would automatically check a box that enrolled consumers in a paid subscription without warning.[31] This case is still ongoing.

These cases illustrate a notable shift: the FTC now explicitly alleges the use of dark patterns in its complaints. This practice occurred significantly less in cases brought prior to the FTC's 2022 report where the term dark patterns was not used to describe the same behaviors.[32] The FTC's new practice of alleging the use of dark patterns explicitly in the complaint illustrates the regulating agencies continuing efforts to crystallize the manipulative and coercive behaviors known as dark patterns to further develop these areas of privacy regulation and consumer protection. The FTC's heightened intensity in regulating dark patterns, coupled with the agency's new practice of explicitly mentioning dark patterns in the complaint, serves as a reminder to companies that the FTC has not backed off its pursuit against these schemes.[33] By continuing to bring more nuanced and sophisticated suits targeting these deceptive and manipulative practices, "the message for other companies should be clear[;]" take steps to avoid employing dark patterns.[34]

---

[27] Complaint at ¶¶ 9-10, *In re Epic Games, Inc.* (F.T.C. March 14, 2023) (No. C-4790), https://perma.cc/F8C9-GRU5 [hereinafter *Epic Games* Complaint].

[28] Fortnite Refunds, F.T.C., FTC is Sending Payments to Fortnite Gamers who were Charged for Unwanted Items (Sept. 2023), https://perma.cc/PEB8-M7VG.

[29] *Publishers* Complaint at ¶¶ 1-3 (alleging the defendant uses dark patterns), *supra* note 12.

[30] Press Release, F.T.C., FTC Takes Action Against Publishers Clearing House for Misleading Consumers About Sweepstakes Entries (June 27, 2023), https://perma.cc/LP56-Y38T.

[31] Complaint at ¶¶ 1, 2, 16-17, *FTC v. Doxo, Inc.* (W.D. Wash. Apr. 25, 2024) (No. 2:24-cv-00569), https://perma.cc/AU2V-RZU3 [hereinafter *Doxo* Complaint].

[32] *Compare* Complaint at ¶¶ 38, 62-67, *FTC v. Age of Learning, Inc.* (C.D. Cal. Sept. 1, 2020) (No. 2:20-cv-07996), https://perma.cc/WN4N-AQ2B (asserting, among other claims, but without using the term dark pattern, that the defendant "failed to provide a simple cancellation mechanism" under ROSCA by requiring users to navigate six to nine screens throughout the process, 15 U.S.C. § 8403), *with* Complaint at ¶¶ 2, 7, *FTC v. Amazon, Inc.* (W.D. Wash. June 21, 2023) (No. 2:23-cv-00932), https://perma.cc/PJR9-7XU5 ("Amazon used manipulative, coercive, or deceptive user-interface designs known as 'dark patterns' to trick consumers into enrolling in automatically-renewing Prime subscriptions" and "knowingly complicated the cancellation process"); *but see* Statement of Commissioner Rohit Chopra, F.T.C., *Regarding Dark Patterns in the Matter of Age of Learning, Inc.* (Sept. 2, 2020), https://perma.cc/7PJN-3LF2.

[33] Chris O'Malley, *FTC Sues Doxo, Signaling 'Dark Patterns' Crackdown Still Underway*, NAT'L L. J. (May 7, 2024), https://perma.cc/4YQV-4Y46.

[34] Lesley Fair, *$245 Million FTC Settlement Alleges Fortnite Owner Epic Games Used Digital Dark Patterns to Charge Players for Unwanted In-Game Purchases*, F.T.C. BUSINESS BLOG (Dec. 19, 2022), https://perma.cc/GWV5-5DLE.

Furthermore, in July of 2024, the FTC and two international consumer protection networks released the findings of a new review that showed, despite all the FTC's recent and high-profile litigation, dark patterns are still pervasive and continue to gain complexity.[35] This further highlights that the FTC has been increasingly prioritizing dark pattern actions over the past several years, and there is no sign this enforcement strategy will slow down.

B. California's Unmistakable Denouncement of Dark Patterns

As the FTC made significant progress along its path of targeting companies who employ dark patterns federally, California kept stride and became the first state to enact comprehensive privacy legislation in 2018 through the California Consumer Privacy Act ("CCPA").[36] The CCPA went into effect on January 1, 2020, and "gives consumers more control over the personal information that businesses collect about them."[37] In doing so, the law grants consumers "the right to know about the personal information a business collects" and "the right to opt-out of the sale" of their personal information.[38] These new privacy rights are the most pertinent sections to regulating dark patterns in the future. Subsequently, California Attorney General, Rob Bonta ("Attorney General Bonta"), "began sending notices of alleged noncompliance to companies beginning on July 1, 2020, when enforcement of the CCPA began."[39] However, because the CCPA does not explicitly use the term dark pattern, none of the notices included this term either.[40] The CCPA, and thus the notices, only addressed situations where a company does not provide consumers the ability to opt-out at all. As a result, enforcement did not extend to the more nuanced practices the Act later covered where companies misled consumers into seemingly opting-in without having truly provided their consent.[41] Hence, this stage in California's development of the increasing scrutiny given to dark patterns mirrors the FTC's starting point.[42]

---

[35] FTC Announces Dark Pattern Results, *supra* note 1.

[36] Cal. Priv. Act of 2018, CAL. CIV. CODE § 1798.100.

[37] *California Consumer Privacy Act (CCPA)*, STATE OF CAL. DEP'T OF JUST. OFF. OF THE ATT'Y GEN. (March 13, 2024), https://perma.cc/T67B-5NHJ.

[38] *Id.*; *see* CAL. CIV. CODE § 1798.185(a)(4)(A) ("To facilitate and govern the submission of a request by a consumer to opt out of the sale of personal information."); CAL. CIV. CODE § 1798.185(a)(6) ("Ensure that the notices and information . . . are provided in a manner that may be easily understood by the average consumer."); CAL. CIV. CODE § 1798.185(a)(4)(A)(C) ("To promote consumer awareness."); CAL. CIV. CODE § 1798.185(a)(7) ("With the goal of minimizing the administrative burden on consumers.").

[39] *CCPA Enforcement Case Examples*, STATE OF CAL. DEP'T OF JUST. OFF. OF THE ATT'Y GEN., https://perma.cc/NMT6-FKNY.

[40] Jennifer King & Adriana Stephan, *Regulating Privacy Dark Patterns in Practice—Drawing Inspiration from California Privacy Rights Act*, 5 GEO. L. TECH. REV. 251, 274 (2021).

[41] Proposition 24 Amends Consumer Privacy Laws. Initiative Statute., LEGIS. ANALYST OFF. (Nov. 3, 2020), https://perma.cc/R4WG-64A5.

[42] *See In re Geocities* Complaint, *supra* note 8.

Key to understanding one of the main goals of the CCPA and its path to explicitly including dark patterns in its text is evaluating how a consumer's right to opt-out of having a company sell or share personal data evolved.[43] This is displayed through amendments added to the CCPA in March of 2021, which forbid tactics such as "using confusing language, requiring a user to input unnecessary information before completing an opt-out request," and "forcing users to click through reasons why they should not submit their data privacy request" prior to being able to opt-out.[44] Hence, these amendments are describing the behaviors of dark patterns while also prohibiting the outcomes and effects they produce, such as the subversion or impairment of a consumer's choice;[45] even so, the term dark pattern was still not included in these amendments.

Attorney General Bonta's interpretation of the CCPA and its subsequent amendments at this point in time is best displayed through the action brought against the company Sephora.[46] In the first enforcement action of the Act, Sephora was charged with violating a "hallmark of the CCPA," a consumer's right to opt-out.[47] Sephora did not provide consumers with any opportunity to opt-out and instead falsely conveyed that it did not sell users personal information.[48] The complaint argues the right to opt-out "requires that companies follow certain straightforward rules: if companies make consumer personal information available to third parties and receive a benefit from the arrangement . . . they are deemed to be 'selling' consumer personal information under the law."[49] Moreover, this act of selling "triggers certain basic obligations," including that the business notify consumers of this practice and "allow consumers to opt-out of those sales, such as by clicking an easy-to-find 'Do Not Sell My Personal Information' link."[50] The strength of this argument compelled Sephora to settle, and the company paid consumers $1.2 million in penalties.[51]

This outcome displays a baseline of how the CCPA may be used to try additional companies in the future. Yet, it also shows that the starting point for litigation under the CCPA—when the term dark pattern was not explicitly used—began with an action for the complete failure to notify and provide

---

[43] *See* Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 B.U. L. REV. 593, 615 (2024).

[44] Jordyn Michaels, *Pathways to the Light: Realistic Tactics to Address Dark Patterns*, 49 RUTGERS COMPUTER & TECH. L.J. 176, 189 (2022).

[45] *See* Sherry-Maria Safchuk & Garylene Javier, *Differences Between the California Consumer Privacy Act and the California Privacy Rights Act*, 74 CONSUMER FIN. L.Q. REP. 400, 408 (2021).

[46] *See* Complaint at ¶ 1, *People of the State of California v. Sephora USA, Inc.* (Sup. Ct. Cal. Aug. 23, 2022) (No. CGC-22-601380), https://perma.cc/N9P4-SYRW [hereinafter *Sephora* Complaint].

[47] *Id.* at ¶ 3.

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] Final Judgment and Permanent Injunction at ¶ 17, *People of the State of California v. Sephora USA, Inc.* (Sup. Ct. Cal. Aug. 24, 2022) (No. CGC-22-601380), https://perma.cc/PA68-KUTS.

consumers with the ability to opt-out of having their personal information sold. Thus, at the CCPA's initial starting point, the litigation did not regard the employment of a more deceptive dark pattern, which, for example, would present a chance to opt-out that requires more steps than it would take to simply provide consent to opt-in.[52] In this way, California's and the FTC's litigation paths progress similarly; prior to California and the FTC beginning to use the term dark pattern explicitly in their complaints, both entities only focused on the complete denial of the ability to opt-out.[53]

In further development of California's consumer privacy laws, California voted to pass the California Privacy Rights Act of 2020 ("CPRA"), which would again amend the CCPA.[54] Among other amendments, the CPRA created a new state agency called the California Privacy Protection Agency ("CPPA"), which will oversee and enforce the Act's privacy laws.[55] Significantly, the CPRA uses the term "dark pattern" numerous times in relation to when consumers exercise their "right to limit the use and disclosure of sensitive personal information."[56] The CPRA defines a dark pattern to be "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice."[57] This amendment to the CCPA further states that "agreement obtained through use of dark patterns does not constitute consent,"[58] specifically noting that the presentment of an option to either opt-in or opt-out must "not make use of any dark patterns."[59] Additionally, the CPRA provides more clarity by including the principles that must be present to obtain consumer consent,[60] such as having options that (1) are "easy to understand," (2) have "symmetry in choice," (3) avoid confusing the consumer, (4) avoid impairing or interfering "with the consumer's ability to make a choice," and (5) are "easy to execute."[61]

All the sections of the CPRA cited above became fully enforceable as of July 1, 2023.[62] Hence, companies should understand they may be investigated by the CPPA, and that the state agency or Attorney General Bonta may take action against them. Where dark patterns used to be a purely academic concept, they are now federally regulated as well as specifically defined and codified in California.

---

[52] Enforcement Advisory No. 2024-02, *Avoiding Dark Patterns: Clear and Understandable Language, Symmetry in Choice*, CAL. PRIV. PROT. AGENCY ENF'T DIV. 1, 3 (Sept. 4, 2024), https://perma.cc/557P-YBVX.

[53] *See* FTC Announces Dark Pattern Results, *supra* note 1.

[54] LEGIS. ANALYST OFF., *supra* note 41.

[55] STATE OF CAL. DEP'T OF JUST. OFF. OF THE ATT'Y GEN., *supra* note 37.

[56] *Id.*

[57] CAL. CIV. CODE § 1798.1401(l).

[58] CAL. CIV. CODE § 1798.140(h).

[59] CAL. CIV. CODE § 1798.185(a)(19)(C)(iii) (July 15, 2024) (amending § 1798.185(a)(20)(C)(iii) (Jan. 1, 2024)).

[60] CAL. CODE REGS. tit. 11 § 7004(a)(5)(B), (C).

[61] *Id.* at § 7004.

[62] *California Consumer Privacy Laws*, BLOOMBERG LAW, https://perma.cc/V36H-BAVU.

C. Prospective Impact on California Businesses

California companies, under the purview of the CCPA, as amended by the CPRA (hereinafter "amended CCPA" for clarity in distinguishing between the different versions),[63] should ensure they are not employing dark patterns. As evidenced by the amended CCPA's evolution, California has been strengthening the requirements that companies must adhere to by expanding upon the rights afforded to consumers.[64]

The amended CCPA is relatively new, and as a result, Attorney General Bonta is still beginning to bring litigation against companies who did not cure violations originally described in the notices sent to businesses when the CCPA was originally enacted.[65] In January of 2020, the first month the CCPA was in effect, DoorDash illegally sold consumers' personal information without providing any notice or an opportunity to opt-out.[66] About four years later, DoorDash settled and agreed to pay $375,000 in civil penalties and to comply with "strong injunctive terms."[67] This marked the second public settlement under the CCPA,[68] which followed Sephora's settlement. While both the Sephora and DoorDash complaints centered around the defendants' failure to provide any notice or opportunity for consumers to opt out of the sale of their personal information,[69] Attorney General Bonta further outlined the contours of the CCPA in the suit against DoorDash by clarifying what may count as a "sale" under the CCPA.[70] DoorDash's behavior was deemed a sale where the company disclosed consumers' personal information as part of its membership in a marketing cooperative in exchange for the ability to reach new customers.[71] Additionally, Attorney General Bonta released stronger remarks compared to Sephora's settlement for how other businesses should interpret the enforcement action taken against DoorDash, stating it should serve "as a wakeup call to businesses: The CCPA has been in effect for over four years now, and businesses must comply with this important privacy law."[72] Nonetheless, even with the amended CCPA in effect, the DoorDash complaint

---

[63] STATE OF CAL. DEP'T OF JUST. OFF. OF THE ATT'Y GEN., *supra* note 37.

[64] Solove, *supra* note 43 (Evaluating that the CCPA, as originally enacted, requires that a privacy notice be clearly posted on an organization's website. The CCPA's first revision goes a step further by mandating a conspicuous button for people to have the ability to opt-out of "selling" their personal data. Then, the amended CCPA goes even further by extending the notification and opt-out requirements to cover the "selling or sharing" of personal data).

[65] *See* STATE OF CAL. DEP'T OF JUST. OFF. OF THE ATT'Y GEN., *supra* note 37.

[66] Complaint at ¶¶ 7-12, *The People of the State of California v. DoorDash, Inc.*, No. CGC-24-612520, 2024 WL 729652 (Sup. Ct. Cal. Feb. 21, 2024) [hereinafter *DoorDash* Complaint].

[67] Press Release, Rob Bonta Attorney General, Attorney General Bonta Announces Settlement with DoorDash, Investigation Finds Company Violated Multiple Consumer Privacy Laws (February 21, 2024), https://perma.cc/UMN8-TNZV [hereinafter *DoorDash* Press Release].

[68] *Id.*

[69] *Compare DoorDash* Complaint, *supra* note 67, *with Sephora* Complaint, *supra* note 46.

[70] *DoorDash* Complaint, *supra* note 67.

[71] *Id.*

[72] *DoorDash* Press Release, *supra* note 68.

displays how original cases are still being tried under the CCPA as it was first enacted. Consequently, while these early cases impact the understanding of language that is still present in the amended CCPA, they do not yet extend to suits against companies who employ more sophisticated dark patterns, which deceptively manipulate consumers into opting-in.

However, the CPPA published an enforcement advisory in September of 2024,[73] and this advisory further adds to the likelihood that California will begin to bring cases explicitly alleging the violation of employing dark patterns within its complaint, similar to when the FTC began doing the same and brought a barrage of cases.[74] The enforcement advisory solely addresses dark patterns and provides a factual scenario to illustrate several examples of common opt-out methods companies present to consumers.[75] The advisory's omission of an answer as to whether or not each example qualifies as a dark pattern indicates it should be extremely clear. Consequently, the advisory is pointing out that these examples are firmly established and should already be well-known and understood by companies.

Additionally, the enforcement advisory highlights that to determine whether a company's opt-out process uses a dark pattern, it will require the company, or the CPPA, to conduct a fact-specific, case-by-case analysis.[76] This evaluation should not only consider the language presented to consumers, but also the design choices such as the message's location, size, color, font size, and the process a consumer faces to successfully opt-out.[77] This further clarification can be seen as notice to businesses and as a sign that the CPPA is looking to continue taking action against companies who blatantly refuse to provide an opt-out option or misinform users about whether personal information is being shared or sold, but also against companies who go a step further and create confusing or complex mechanisms to trap consumers into being unable to truly provide their consent.

The urgency for companies to ensure their opt-out notices and requests comply with the amended CCPA, and the specific characteristics outlined in section 7004 of the California Code of Regulations,[78] is reinforced by the elimination of the thirty-day cure period originally present in the CCPA.[79] While the CPPA still maintains the discretion to permit businesses to cure alleged violations,[80] the removal of the thirty-day cure period likewise takes away a company's ability to argue it made a good-faith effort to cure the alleged

---

[73] CAL. PRIV. PROT. AGENCY ENF'T DIV., *supra* note 52.

[74] *See Epic Games* Complaint, *supra* note 27; *Publishers* Complaint, *supra* note 12; *Doxo* Complaint, *supra* note 31.

[75] CAL. PRIV. PROT. AGENCY ENF'T DIV., *supra* note 52.

[76] *Id.*

[77] *Id.*

[78] CAL. CODE REGS. tit. 11 § 7004.

[79] The cure provision previously appeared in CAL. CIV. CODE § 1798.155(b).

[80] CAL. CIV. CODE § 1798.199.45.

violation prior to the start of litigation. This not only reduces the likelihood that the CPPA may exercise its discretion in granting a cure period; it also factors into the civil penalty a company may receive if the allegations are found to be true. The amended CCPA states a business may be liable up to $2,500 for each violation of the Act or $7,500 for each intentional violation of the Act.[81] As part of Attorney General Bonta's statement following DoorDash's settlement, he stressed that "violations cannot be cured," and the office will be holding "businesses accountable."[82] Hence, the removal of this more business-friendly provision, in conjunction with the publication of the enforcement advisory, should be understood as the CPPA indicating that companies have already received notice and the agency will soon begin targeting businesses who employ dark patterns, similar to the FTC, swiftly and with full force.

As the CPPA begins to start bringing cases under the amended CCPA, the question of what the outer bounds of a more sophisticated or complex dark pattern exactly resembles should likely start to gain additional clarity. While it is useful for states to look to one another,[83] California typically leads other states in implementing privacy laws as the state is traditionally the strongest protector of consumer rights. As a result, the term "California effect" has been coined to explain the phenomenon where businesses that operate across multiple jurisdictions will comply with the strictest set of laws and regulations because it is expensive to treat consumers in different jurisdictions differently.[84] In most areas, California is regarded as the leader and is "a major force in data privacy law."[85] For example, the CCPA distinguishes itself from all other state privacy laws by not only requiring "opt-in consent for the processing of sensitive data," but also specifying "that mechanisms for giving or revoking consent may not be presented via a pop up, banner, or other intrusive design, and may not require the consumer to state a preference in order to receive full functionality to the website."[86] Hence, as California is currently a leader in consumer privacy laws and the codification of dark patterns, California businesses should look to the FTC's actions to gauge where Attorney General Bonta and the CPPA are heading next.

Notably, however, the amended CCPA may be viewed as a more comprehensive framework for bringing suits against companies that employ

---

[81] CAL. CIV. CODE § 1798.199.90.

[82] *DoorDash* Press Release, *supra* note 68.

[83] As of September 10, 2024, twenty states have enacted comprehensive consumer data privacy laws. *Which States Have Consumer Data Privacy Laws?*, BLOOMBERG LAW (Sept. 10, 2024), https://perma.cc/L82M-R46X; *see, e.g.*, Colorado Privacy Act, COLO. REV. STAT. §§ 6-1-1201-13 (2023); Virginia Consumer Data Protection Act, VA. CODE ANN. §§ 59.1-575-85 (2024); Oregon Consumer Privacy Act, S. 619, 82d Leg. Assemb., Reg. Sess. (Or. 2023).

[84] Jens Frankenreiter, *Is there a "California Effect" in Data Privacy Law? Why the EU is Not the World's Privacy Cop*, PROMARKET (Oct. 21, 2021), https://perma.cc/L82M-R46X.

[85] *Id.*

[86] Maureen E Fulton & Mikaela M. Witherspoon, *What are Dark Patterns?*, KOLEY JESSEN (Aug. 1, 2024), https://perma.cc/BHZ7-5TSC.

dark patterns compared to the FTC's because the amended CCPA specifically defines the practice[87] and outlines the characteristics companies must incorporate into their behaviors to be deemed to have obtained consumer consent.[88] In contrast, the FTC Act only sets forth a broad prohibition of "unfair" or "deceptive" practices.[89] Thus, California's explicit codification that dark patterns are a violation of the amended CCPA also indicates the states' ability to take a firmer stance against the more nuanced forms of dark patterns. Attorney General Bonta indicated the state would be doing just this in a press release soon after the conclusion of DoorDash's settlement announcement.[90] Bonta stated that he would be directing his attention towards streaming services' compliance with the amended CCPA.[91] In doing so, Bonta stressed the amended CCPA requires that businesses provide consumers the right to opt-out of the selling or sharing of their data and personal information.[92] Importantly, however, he also stated that "exercising this right should be easy and involve minimal steps."[93] This statement is directly meant to encapsulate the behaviors known as dark patterns. Further, Bonta also stated that a consumers' opt-out request should not only be easy, but that it should also include further options, such as the ability to "have this choice honored across different devices."[94] For example, if a user is logged into Netflix on their television and opts-out of allowing their personal data to be shared and sold, then this decision should also be mirrored when the user accesses Netflix on their phone. This shows the state is no longer in its initial enforcement phase in bringing suits similar to Sephora and DoorDash for failing to provide consumers the ability to opt-out completely. Instead, similarly to the FTC's path, Attorney General Bonta is intending to begin targeting businesses, particularly streaming services, that employ the more nuanced, deceptive, and manipulative behaviors encapsulated by the term "dark pattern" as used in the amended CCPA. However, all businesses, not merely streaming services, should be alert to California's enforcement of the amended CCPA as the CPPA is likely to begin bringing cases against companies more broadly for their use of these more nuanced forms of dark patterns.

---

[87] CAL. CIV. CODE § 1798.140(l).

[88] CAL. CODE REGS. tit. 11 § 7004.

[89] 15 U.S.C. § 45(a)(1).

[90] Press Release, Rob Bonta Attorney General, Attorney General Bonta Announces Investigative Sweep, Focuses on Streaming Services' Compliance with the California Consumer Privacy Act, https://perma.cc/A3A4-8TBG.

[91] *Id.*

[92] *Id.*

[93] *Id.*

[94] *Id.*

III. CONCLUSION

The previous actions brought in court and the publication of enforcement advisories display how dark patterns may emerge in several different areas of consumer protection law. The FTC's and California's paths include examples that range from when a company does not disclose its personal information collection policy at all to when a company coerces consumers to opt-in without actually having provided their consent. In addition, behaviors and practices such as not providing a clear and straightforward opt-out procedure, even in cases where consumers did originally consent to opting-in, will likely see future enforcement that alleges the company violated the amended CCPA by alleging the business illegally employed a dark pattern directly in the complaint. The increasing enforcement attention at all levels indicates that dark pattern enforcement is no longer in its early stages and is instead establishing itself as a rapidly growing body of law that has a clear prohibition on manipulating and deceiving consumers.

In evaluating what California businesses may expect from how the CPPA will coordinate its efforts with Attorney General Bonta, companies should keep a close eye on which cases the FTC decides to pursue. California, being a leader in consumer privacy laws, will likely follow the FTC's lead, rather than another state. Given that the FTC began by targeting companies who completely failed to provide an opt-in or opt-out option and then progressed to pursuing cases that coerced consumer consent or trapped consumers into previously entered agreements, California, having only brought the former types of cases up to this point, is likely to begin taking action against companies that use the latter, more nuanced, schemes. However, it is important to note that if the FTC does not pursue, or fully pursue, certain types of cases, California may still choose to target additional deceptive or manipulative practices the state sees as impairing consumer autonomy by bringing action under the amended CCPA because it codifies the violation of employing dark patterns. As California continues to lead in shaping and enforcing robust consumer privacy protections, businesses must recognize that increasingly sophisticated dark pattern schemes will face heightened scrutiny from both Attorney General Bonta and the CPPA.