Published on *The National Law Review* https://natlawreview.com

Dark Patterns Come to Light in California Data Privacy Laws

Article By:

Jeremy Merkel

Imagine this scenario: You are navigating through a website or watching an in-app ad, when suddenly you are redirected to a subscription page, even though you have no interest in the product being marketed to you. Later on, you come across a platform that you actually want to use, but in order to do so, you are required to sign up for a seven-day free trial. Unbeknownst to you, after the free trial period ends, you are charged a subscription fee. When you try to cancel the subscription, the website or app forces you to click through multiple screens, scroll through numerous panes, and check several boxes to do so. Instead of going through the arduous process, you abandon the task and continue paying for the subscription.

If these online experiences sound familiar to you, you are one of countless consumers who has been a victim of a dark pattern.

What are Dark Patterns?

Dark patterns are features of interface design deployed by websites or apps for the purpose of influencing users' online behavior and tricking them into making decisions they may not make otherwise, which benefits the business in question. While the tactics are not always as insidious as the name suggests and may not have malicious intent, they are generally carefully crafted based on human psychology, often to coerce and manipulate.

Harry Brignull, the UK-based user experience designer who coined the term "dark patterns" in 2010, describes different types of dark pattern tactics that are commonly used across the internet. Some examples include (1) price comparison prevention, where a retailer makes comparing the prices of different products so difficult that you cannot make an informed decision; (2) misdirection, where the UX design purposefully focuses your attention on one thing in order to distract you from something else; (3) "confirmshaming," the act of guilting you into optingin to a service or providing information; (4) disguised ads, which are advertisements that are disguised as other content or navigation in order to get you to click on them; and (5) the infamous "roach motel," where you can easily sign up for a service, but the business makes it unreasonably complicated to cancel.

When it comes to the roach motel, as the saying goes, "roaches check in, but they don't check out." Drawing upon this allegory, researchers from the Norwegian Consumer Council (Forbrukerrådet) studied Amazon's use of dark patterns to manipulate users into continuing their Amazon Prime

subscriptions, even when they intended to cancel, and published their findings in a report in January.[1] The conclusions served as the basis for a complaint by the internet privacy watchdog, the Electronic Privacy Information Center (EPIC), to the Office of the Attorney General of the District of Columbia, alleging that Amazon's use of dark patterns constitutes an unfair and deceptive trade practice in violation of the D.C. Consumer Protection Procedures Act and the Federal Trade Commission Act.[2]

While calls for regulatory investigations and public reproach (for example, Brignull's website, www.darkpatterns.org, exposes companies that employ dark patterns on its "Hall of Shame") aim to enjoin businesses from profiting off dark patterns and inflict reputational damage on them, US laws have not specifically addressed dark patterns, until now.

The California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)

As is often the case with consumer protection, California is the first state to regulate dark patterns. Regulations approved in March by California's Office of Administrative Law amended the existing CCPA regulations by banning the use of dark patterns to subvert or impair the process for consumers to optout of the sale of personal information. As former California Attorney General Xavier Becerra noted in one of his final press conferences as the state's top law enforcement official, "these protections ensure that consumers will not be confused or misled when seeking to exercise their data privacy rights." The final regulations offered a few illustrative examples of the confusing or excessive designs that are prohibited[3]:

1. The business's process for submitting a request to opt-out can't require more steps than the business's process for a consumer to opt-in to the sale of personal information after having previously opted out. The number of steps for submitting a request to opt-out is measured from when the consumer clicks on the "Do Not Sell My Personal Information" link to completion of the request. The number of steps for submitting a request to opt-in to the sale of personal information is measured from the first indication by the consumer to the business of their interest to opt-in to completion of the request.

2. A business can't use confusing language, such as doublenegatives (e.g., "Don't Not Sell My Personal Information"), when providing consumers the choice to opt-out.

3. Except as permitted under the regulations, a business can't require consumers to click through or listen to reasons why they should not submit a request to opt-out before confirming their request.

4. The business's process for submitting a request to optout cannot require the consumer to provide personal information that is not necessary to implement the request.

5. When a consumer clicks the "Do Not Sell My Personal Information" link, the business shall not require the consumer to search or scroll through the text of a privacy policy or similar document, or webpage to locate the mechanism for submitting a request to opt-out.

Like other violations under the CCPA, businesses that use dark patterns in violation of the regulations have a 30-day cure period to revamp their website or app design. Failure to comply may result in civil penalties brought by the California Attorney General under the CCPA and unfair competition laws.

The CPRA, approved by California voters last November and set to take effect January 1, 2023, goes a step further than the CCPA to affirmatively regulate dark patterns, stating that "consent obtained through dark patterns does not constitute consent"[4] and 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."[5] The rules that could clarify which dark patterns negate consent will be determined by the new California Privacy Protection Agency that is set to convene later this year.

(Failed) State and Federal Bills

Beyond California, privacy bills that would have regulated dark patterns have failed to mobilize. The third iteration of the Washington Privacy Act (S.B. 5062), which included a similar provision to the CPRA, failed to advance before the end of Washington's legislative session. Likewise, a bi-partisan bill introduced in 2019 by Senators Mark Warner and Deb Fischer, the Deceptive Experiences To Online Users Reduction (DETOUR) Act, would have banned internet platforms with more than 100 million users from using any tactics (though it did not refer to them as "dark patterns") that trick users into providing their personal information. The bill never received a vote in the Senate.

Federal Trade Commission (FTC) Enforcement

A recent statement by FTC Commissioner Rohit Chopra signaled that the Commission may be shifting towards a more activist approach for stamping out the use of dark patterns. Acknowledging that the Commission's "whack-a-mole" strategy on hot-button issues like fake reviews, digital disinformation and data privacy may have fallen short of its intended objectives, Commissioner Chopra called on the Commission to deploy all the tools at its disposal in pursuing businesses that trick and trap consumers through dark patterns.[6] The FTC's enforcement actions against businesses using dark patterns saw the culprits incorporating other unlawful practices that are addressed by existing federal laws. Examples include the Restore Online Shoppers' Confidence Act,[7] which requires clear and conspicuous disclosures of key terms and "simple mechanisms" to stop recurring charges, as well as a statute that digital marketers may be all too familiar with, the CANSPAM Act, which prohibits deceptive header information and requires marketers to provide email recipients a simple way to opt out of future emails.[8]

Further signaling its commitment to protecting consumers from online manipulation, on April 29, the FTC hosted a multidisciplinary workshop entitled, "Bringing Dark Patterns to Light." Among the topics covered, panelists discussed the factors and incentives that give rise to dark patterns, the effects that dark patterns have on consumer choices and behavior regarding privacy, purchasing, and content selection, and how educational, technological, and self-regulatory solutions have the potential to mitigate dark patterns' effects. The workshop also delved into more nuanced discussions, such as research findings on consumers' reactions to graduated levels of dark patterns aimed at manipulating them into paying for unwanted identity theft protection services, and how minority communities and minors are particularly susceptible to dark patterns.

What's Next for Dark Patterns?

While the concept of dark patterns isn't new or novel, the CCPA, CPRA, and FTC have resurrected it as an issue of substantial regulatory risk. For businesses maintaining an interactive website or app, being cognizant of the design elements that could be considered dark patterns, with a particular emphasis on features that collect personal information or attempt to obtain user consent, is a logical

place to begin assessing compliance. Businesses may also, as part of their own privacy-by-design programs, allow key user interface areas or information collection mechanisms to be reviewed by a neutral personnel or a third party auditor. Monitoring legal developments, like the CPRA's rulemaking proceedings, could be helpful for businesses in preparing for dark pattern regulations. Until then, streaming the FTC's workshop on dark patterns is a great place to start.

---

1. Forbrukerrådet, You Can Log Out, but You Can Never Leave (Jan. 14, 2021)

2. In the Matter of Amazon.com, Inc., EPIC Complaint, Office of the Attorney General for D.C., February 23, 2021

3. Cal. Code Regs. Tit. 11, Div. 1, Chap. 20 § 999.315(h).

4. Cal. Civ. Code § 1798.140(h)

5. Cal. Civ. Code § 1798.140(l).

6. Statement of Commissioner Rohit Chopra Regarding Dark Patterns in the Matter of Age of Learning, Inc. *Commission File Number 1723186,* September 2, 2020.

7. 15 U.S.C. §§ 8401–05.

8. 15 U.S.C. § 7704(a).

National Law Review, Volume XI, Number 183

Source URL:https://natlawreview.com/article/dark-patterns-come-to-light-california-data-privacy-laws