



Hot Topics in Privacy Enforcement: Key Trends in FTC, State, and Private Enforcement

Presented by

D. Reed Freeman, Jr.
Partner, ArentFox Schiff
Reed.Freeman@afslaw.com

Michelle R. Bowling
Associate, ArentFox Schiff
Michelle.Bowling@afslaw.com

Privacy Spotlight: Opt-Out Preference Signals and Dark Patterns

1. Overview of Comprehensive U.S. State Privacy Laws
2. Deep Dive: Opt-Out Preference Signals
3. Deep Dive: Dark Patterns

Overview of Comprehensive U.S. State Privacy Laws

This year, we will see five U.S. state privacy laws take effect.

Effective January 1, 2023

- The California Privacy Rights Act (“CPRA”), which amends the California Consumer Privacy Act (“CCPA”)
- Virginia Consumer Data Protection Act (“CDPA”)

Effective July 1, 2023

- Colorado Privacy Act (“CPA”)
- Connecticut Act Concerning Personal Data Privacy and Online Monitoring (“CTDPA”)

Effective December 31, 2023

- Utah Consumer Privacy Act (“UCPA”)

State Privacy Laws Recently Passed Laws

Four additional comprehensive privacy laws were also recently passed:

- **Montana Consumer Data Protection Act*** – Effective October 1, 2024
- **Iowa (Senate File 262)** – Effective January 1, 2025
- **Tennessee Information Protection Act** – Effective July 1, 2025
- **Indiana Consumer Data Protection Act** – Effective January 1, 2026

*Awaiting enactment by Governor.

State Privacy Laws

Consumer Rights

Depending upon the state of residence, consumers may have the following rights:

- Right to access
- Right to confirm personal information processing
- Right to data portability
- Right to deletion
- Right to correction of inaccuracies/right of rectification
- Right to opt-out/object to automated decision-making
- Right to opt-out of profiling (in furtherance of decisions that produce legal or similarly significant effects)
- Right to opt-in to the collection/use of sensitive personal information
- **Right to limit the use or disclosure of sensitive personal information (where used to infer characteristics about consumer)**
- **Right to opt-out of “sale” of personal information**
- **Right to opt-out of targeted advertising/”sharing” for cross-contextual behavioral**

State Privacy Laws Right to Opt-Out of a “Sale”



All 5 laws allow consumers the right to opt-out of a “sale” of personal information.

- **CA, CO, CT:** define a “sale” as an exchange for **monetary or other valuable consideration**.
- **VA and UT:** define a “sale” as an exchange for **monetary consideration only**.

State Privacy Laws Right to Opt-Out of Sharing/Targeted Advertising

CA: Provides the right to opt-out of “sharing” for the purposes of cross contextual advertising, defined as the **processing of a consumer’s personal information across businesses or distinctly branded websites/ applications for the purposes of targeted advertising.**

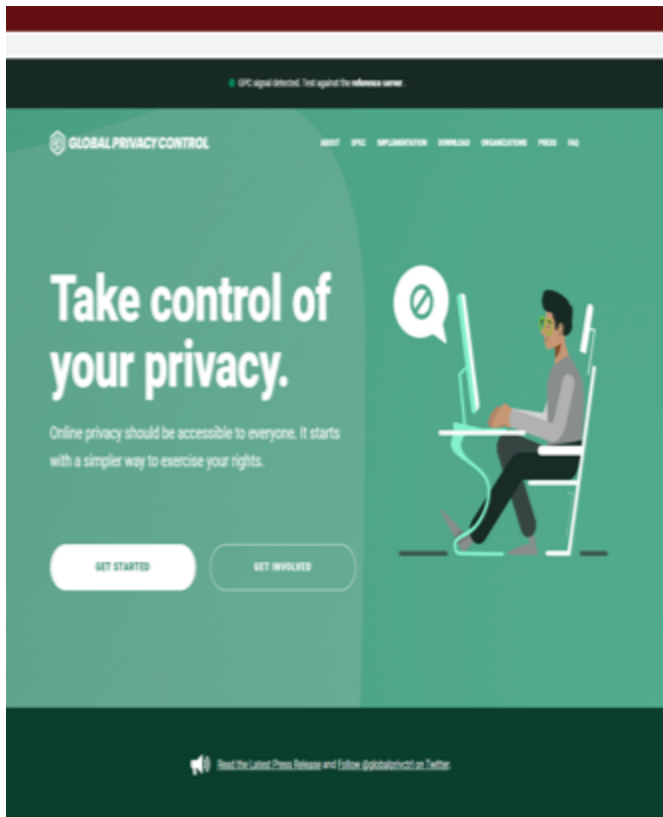
CO, CT, VA, UT: These states provide consumers with the right to opt-out of “targeted advertising” which is **defined similarly to California’s cross-contextual behavioral advertising.**

Deep Dive: Opt-Out Preference Signals

Which states require opt-out preference signals to be honored?

- **California** In effect now!
- **Colorado** July 1 ,2024
- **Connecticut** January 1, 2025

Opt-Out Preference Signals Definition



- A signal sent by a platform, technology, or mechanism on behalf of the consumer that **communicates a consumer’s choice to opt-out of a sale or targeted advertising/ sharing of personal information for cross-contextual advertising.**
- May also be used by consumers as a request to limit the use of sensitive personal information under CCPA.
- A.k.a. global privacy controls (“GPC”) or universal opt-out mechanisms (“UOOM”).
- California Attorney General has endorsed the Global Privacy Control, and CO and CT are likely to do the same.

Depending upon the jurisdiction, these signals are meant to provide a simple and easy-to-use method by which consumers interacting with businesses online can automatically exercise certain opt-out rights with all businesses they interact with online **without having to make individualized requests** to each business.

Opt-Out Preference Signals California Consumer Privacy Act (“CCPA”) Requirements

- CCPA Regulations require businesses to **treat these signals as valid opt-outs of sale/sharing/targeted advertising for that browser or device, and if known, the consumer.**
- Consumers may also use opt-out preference signals as a **request to limit the use or disclosure of their sensitive personal information** (where used to infer characteristics about the consumer).

Opt-Out Preference Signals CCPA Requirements, Cont'd.

- **Businesses must process any opt-out signal that meets the following requirements:**
 - The signal shall be in a format commonly used and recognized by businesses, such as HTTP header or JavaScript object.
 - The platform, technology, or mechanism that sends the opt-out preference signal must make it clear to the consumer that its effect will be an opt-out from the sale and/or sharing.
- **How to implement these signals** must be disclosed in the business's Privacy Policy.
- Opt-out preference signals may be used in lieu of the "Do Not Sell or Share My Personal Information," "Limit the Use of My Sensitive Personal Information" or Alternative Opt-out link(s), as long as they are honored in a frictionless manner.

Opt-Out Preference Signals CCPA Requirements, Cont'd.

Honoring signals in a “**frictionless manner**” means that businesses shall not:

- 1) charge a fee or require any valuable consideration if the consumer uses the signal;
- 2) change the consumer’s experience with the product or service offered by the business; and
- 3) display any notification, pop-up, text, graphic, animation, sound, video or other interstitial content in response to the signal unless it’s a display of whether the consumer has opted out of the sale/sharing or the business is providing a link to a privacy settings page, menu, or interface that enables the consumer to consent to the business ignoring the signal (subject to some limitations).

Opt-Out Preference Signals Consent

- Businesses must wait 12 months before requesting consent after opt-out of sale/sharing or request to limit use/disclosure of sensitive personal information.
- **Exception:** The CCPA allows businesses that recognize opt-out preference signals to **provide a link to a web page** that enables the consumer to consent to the business ignoring the signal, provided that:
 - 1) The web page **allows consent to be easily revoked** by the consumer or the consumer's representative;
 - 2) The link to the web page **does not degrade the consumer's experience** on the web page the consumer intends to visit and has a similar look, feel, and size relative to other links on the same web page;
 - 3) The consent web page **complies with technical specifications set forth in regulations** adopted pursuant to California Privacy Protection Agency Regulations.
- Where the consumer is known to the business, the absence of an opt-out signal where one was previously sent is not considered consent.

Opt-Out Preference Signals Conflicting Settings

- **If the signal conflicts with a business-specific setting** allowing the business to sell or share personal information, the signal must be considered a valid opt-out but the business may notify the consumer of the conflict and provide the consumer with the opportunity to consent. After consent, the signal can be ignored as long as the consumer is known to the business.
- **If the signal conflicts with a Financial Incentive Program (“FIP”)** that requires the consumer to consent to the sale/sharing of personal information, the business may notify the consumer regarding the conflict and confirm the signal as an intent to withdraw from the FIP.
 - *Consumer affirms request:* signal must be treated as an opt-out of sale/sharing and withdrawal of FIP.
 - *No response:* If the consumer is known to the business, the signal can be ignored with respect to consumer’s participation in FIP.

Q: What if we already recognize Do Not Track?

A: Unclear as to whether these signals will replace Do Not Track, so plan to comply with both.

Q: Is a cookie banner sufficient?

A: No. The CCPA regulations state that cookie banners seeking acceptance of web cookies **do not meet the requirements to enable opt-out requests** under the CCPA because cookies concern the collection of personal information and not its sale or sharing.

Q: Can we have all vendors sign a contract so they're considered service providers or contractors so there is no "sale" or "sharing"?

A: Providing cross-contextual behavioral advertising is not a permitted business purpose under the CCPA, so service providers or contractors performing this on a business's behalf would still be considered third parties.



Universal Opt-Out Mechanisms Colorado Privacy Act (“CPA”) Requirements

- As of **July 1, 2024, Colorado** controllers (businesses) that process personal data for **targeted advertising or sales** must allow consumers to opt out via these signals.
- The Colorado Privacy Act’s refers to these as “**universal opt-out mechanisms**” (“UOOMs”) and its Rules contain prescriptive compliance requirements for honoring UOOMs.
- By January 1, 2024, an approved public list of UOOMs will be released by the CO State Dept. of Law.



Universal Opt-Out Mechanisms Technical Specifications

- The UOOM must align with technical specifications, rules, opinion letters, and interpretive guidance issued by the Colorado Attorney General.
- Any UOOM offered must make clear to the consumer, whether in configuration or through disclosure to the public (such as in a privacy policy):
 - that its purpose is to allow the consumer to opt-out of targeted advertising and/or the sale of personal data; and
 - whether it applies to only a single browser or device.
- Like CCPA, must conform to format commonly used by controllers, such as HTTP or JavaScript.
- UOOM must store, process, or transmit data using reasonable data security measures.

Universal Opt-Out Mechanisms Consent

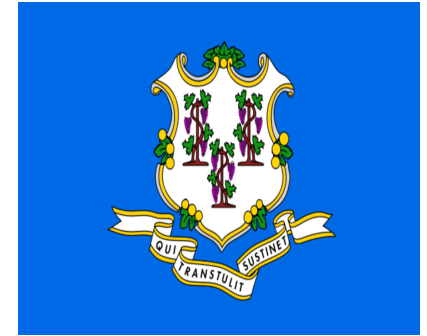


- Unlike CA, the UOOM must “clearly communicate a Consumer’s affirmative, freely given, and unambiguous choice to opt out.”
 - Pre-installed UOOM cannot default to “privacy friendly” opt-out.
- **Controllers can allow a consumer to consent** to targeted advertising or the sale of personal data via a web page, application, or similar method, and that consent will take precedence over choices indicated through UOOM.
- **Absence of a UOOM after consumer’s prior opt-out using UOOM is not consent to opt-in.**
- Consent requests cannot cause “consent fatigue” using pop-ups, interstitial banners, or other mechanisms that degrade or obstruct consumer experience.

Universal Opt-Out Mechanisms Honoring Signals



- **Controller cannot require the collection of additional personal data beyond what is strictly necessary to authenticate the consumer's opt-out request *unless* the controller offers a way to recognize the consumer's UOOM across platforms, devices, or offline.**
- No requirement to authenticate that a resident is a resident of Colorado.
- Data collected via UOOM can only be used to process opt-out preferences.

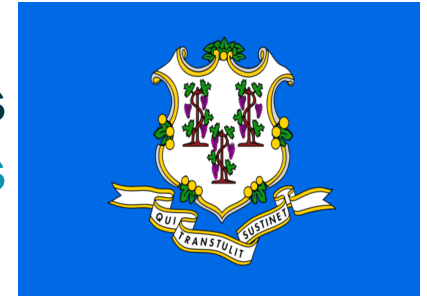


Opt-Out Preference Signals

Connecticut Act Concerning Personal Data Privacy and Online Monitoring

- On January 1, 2025, consumers must be provided with the ability to opt-out of the processing of **personal data for targeted advertising or from the sale of personal data** through an opt-out preference signal.
- Like CO, consumers must make an affirmative choice, so opt-out settings cannot be the default.

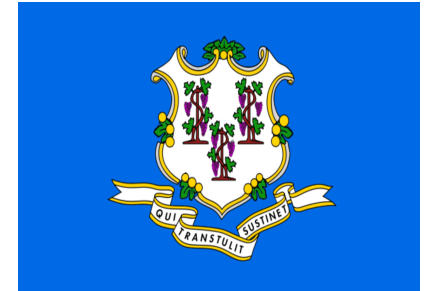
Opt-Out Preference Signals Technical Requirements



Technical specifications require that signals:

- Cannot disadvantage another controller;
- Must be easy to use by the average consumer;
- Must enable the controller to **accurately determine whether the consumer is a CT resident and that this is a legitimate opt-out request**; and
- Consistent with specifications required by any federal or state law or regulation.

Opt-Out Preference Signals Conflicts and Consent



- As with the CCPA, the CTDPA states that **if the signal conflicts with a consumer's voluntary participation in a bone fide loyalty program, rewards, premium features, discounts or club card program** that requires the consumer to consent to the sale of personal information, the business may notify the consumer regarding the conflict and confirm the signal as an intent to withdraw from the program.
- There is no guidance as to whether the signal should be treated as an opt-out pending confirmation of consumer's intent to withdraw from the bona fide loyalty program.

Opt-Out Preference Signals Recent Enforcement



- **Sephora:** The first CCPA enforcement action by the California Attorney General was against Sephora in August 2022. Among the allegations was that Sephora failed to respond to opt-out preference signals as valid consumer opt-out requests. **Sephora settled for \$1.2 million.**
- **Investigative Sweeps:** In late January 2023, the California Attorney General released a statement that his office had completed an “investigative sweep” of popular mobile applications in retail, travel, and food service industries that resulted in businesses receiving letters regarding their noncompliance. One area identified was the **failure of businesses to process opt-out and data deletion requests**, especially those sent via privacy tools, such as the Global Privacy Control, or via authorized agents.

Opt-Out Preference Signals Key Takeaways

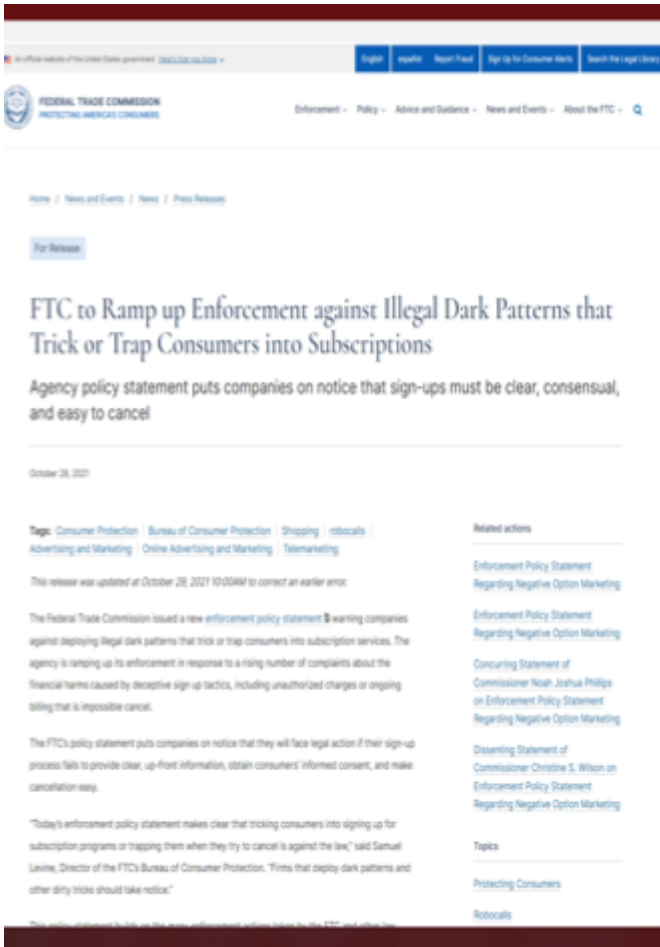
- ✓ Determine whether your organization:
 - “sells;”
 - “shares” for cross contextual behavioral advertising;
 - engages in targeted advertising; and/or
 - uses sensitive personal information for the purposes of creating a profile about a consumer.

- ✓ Ensure your business can honor data subject requests.

Deep Dive: Dark Patterns



The CCPA/CPRA 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.**”



The screenshot shows the FTC website with a press release titled "FTC to Ramp up Enforcement against Illegal Dark Patterns that Trick or Trap Consumers into Subscriptions". The release is dated October 28, 2021, and discusses the agency's policy statement regarding deceptive sign-up tactics. The text includes: "The Federal Trade Commission issued a new enforcement policy statement warning companies against deploying legal dark patterns that trick or trap consumers into subscription services. The agency is ramping up its enforcement in response to a rising number of complaints about the financial harms caused by deceptive sign-up tactics, including unauthorized charges or ongoing billing that is impossible to cancel." and "Today's enforcement policy statement makes clear that tricking consumers into signing up for subscription programs or trapping them when they try to cancel is against the law," said Samuel Levine, Director of the FTC's Bureau of Consumer Protection. "Firms that deploy dark patterns and other dirty tricks should take notice."

- **Section 5 of the FTC Act prohibits “unfair or deceptive acts or practices in or affecting commerce.”** Using this authority, the FTC has brought hundreds of privacy and data security cases.
- In October 2021, the FTC released an enforcement policy statement on **“trick or trap” dark patterns**, which are methods used to induce consumers into signing up for subscription programs and then making it difficult for the consumer to cancel. This was followed by the FTC pursuing settlements against companies that renewed memberships without consent.

Dark Patterns: FTC Enforcement, Cont'd.

In September 2022, the **FTC issued a report** called [“Bringing Dark Patterns to Light”](#) in which it highlighted **four of the most common dark pattern tactics** employed by companies, including:

1. Difficulty in canceling subscriptions or charges

- The FTC has filed actions against companies that **required users to navigate multiple screens** in order to cancel subscriptions.

2. Misleading consumers and disguising advertisements

- Designing advertisements to look like independent editorial content. FTC states that even adding disclaimers to fake editorial content are **unlikely to overcome a “deceptive net impression.”**
- ***Effen Ads – December 2019.*** Operators of a work-from-home scheme sent unsolicited emails to consumers that included “from” lines that falsely claimed they were coming from CNN or Fox News and also routed to fake online news stories that eventually routed to Effen Ads’ sales websites. Operators agreed to a **\$1.5 million settlement.**

Dark Patterns: FTC Enforcement, Cont'd. & Class Actions

3. Hiding key terms and “junk fees”: *Vonage* – November 22

- The FTC alleged that Vonage, an internet phone service provider, **subjected its customers to dark patterns and junk fees** when trying to cancel the services. Vonage was required to revise its T&Cs and simplify the cancellation process.
- Includes “**drip pricing**” in which companies advertise only part of a product’s total price to lure in consumers, and don’t mention mandatory charges until very late in the buying process. (Lending Club)

4. Tricking consumers into sharing unnecessary data

- This tactic, which is also the **highest enforcement priority** for the FTC, employs dark patterns which appear to provide consumers with a choice but intentionally steer them towards an option that provides the most personal information.

Class actions:

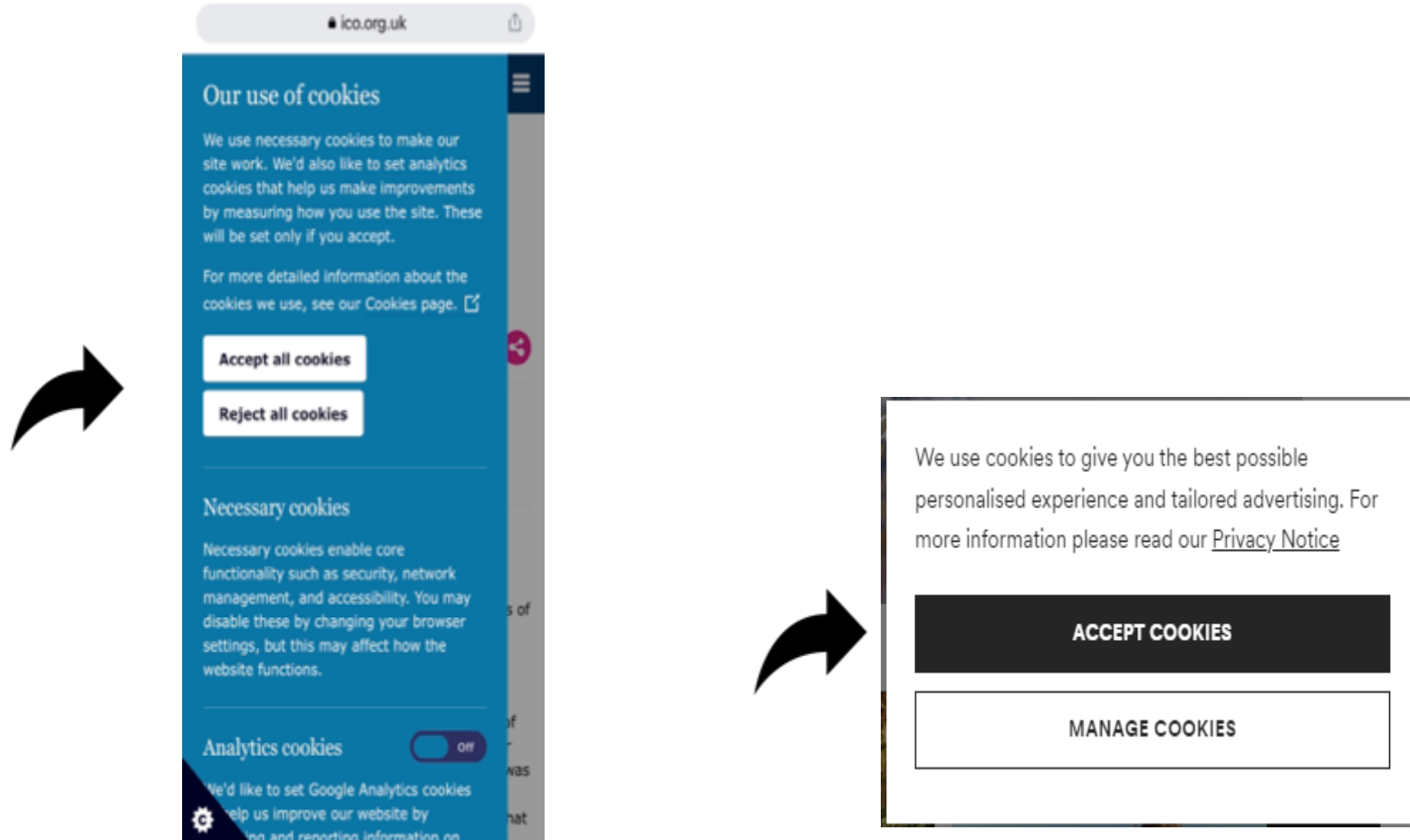
- Noom, which provides a weight loss app, settled a consumer fraud class action in New York for **\$62 million** in which it was alleged that Noom misled customers into signing up for low-cost trial subscriptions that led to expensive, difficult to cancel subscriptions. A former senior software engineer for Noom admitted that **cancelling was “difficult by design,”** a tactic used to generate revenue from consumers that failed to cancel in time to avoid charges.

Dark Patterns: U.S. State Regulation

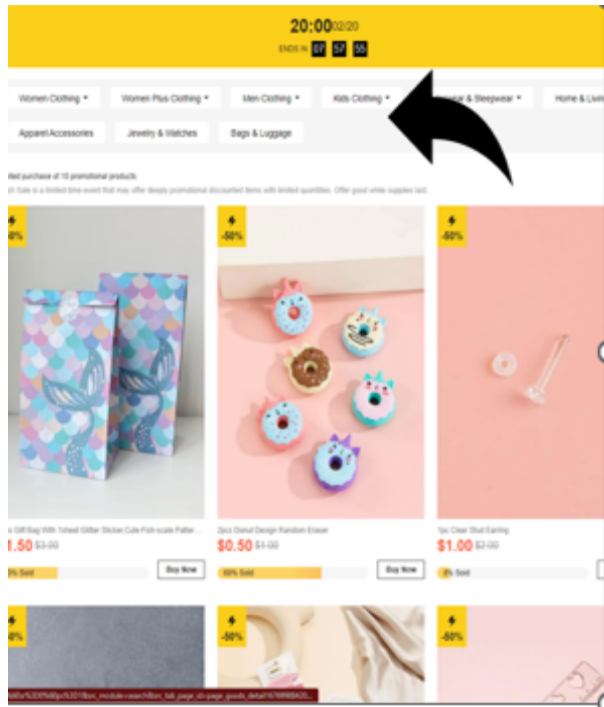
California and Colorado have led the way, outlining methods for submitting consumer rights requests and obtaining consumer consent, which must meet the following requirements or risk being considered a dark pattern:

- **Easy to understand**
- **Symmetry of choice**
 - **Example 1:** Choice to opt-in to sale of personal information. Choices “Yes” and “Ask Me Later” are not symmetrical. “Yes” and “No” are symmetrical.
 - **Example 2:** Website cookie banner provides choices when seeking consent. “Accept All” and “More Choices” are not symmetrical. “Accept All” and “Decline All” are symmetrical.
- **Avoid language that is confusing to the consumer.**
 - **Example:** Double negatives such as choice of “Yes” or “No” next to “Do Not Sell or Share My Personal Information.”

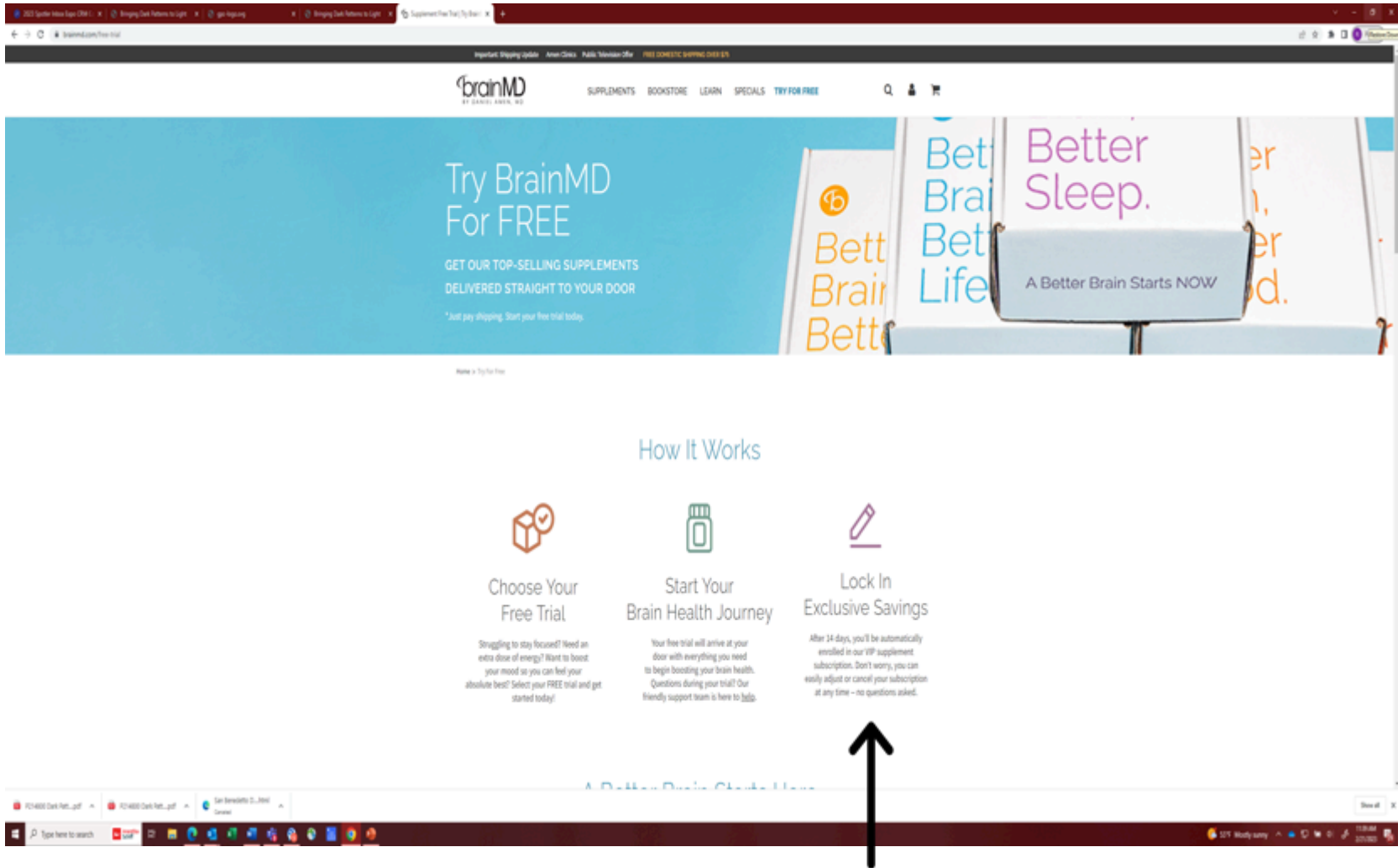
Dark Patterns: Examples



Dark Patterns: Examples



Dark Patterns: Examples



The screenshot shows the BrainMD website with a prominent blue banner for a free trial. Below the banner is a 'How It Works' section with three steps:

- Choose Your Free Trial:** Struggling to stay focused? Need an extra dose of energy? Want to boost your mood so you can feel your absolute best? Select your FREE trial and get started today!
- Start Your Brain Health Journey:** Your free trial will arrive at your door with everything you need to begin boosting your brain health. Questions during your trial? Our friendly support team is here to help.
- Lock In Exclusive Savings:** After 14 days, you'll be automatically enrolled in our VIP supplement subscription. Don't worry, you can easily adjust or cancel your subscription at any time -- no questions asked.

A black arrow points to the 'Lock In Exclusive Savings' step, highlighting a potential dark pattern where users are automatically enrolled in a subscription after the trial period.

- **Avoid choice architecture that impairs or interferes with the consumer's ability to make a choice.**

- **Examples of what to avoid:**

- Requiring consumers to click through multiple screens.
- Bundling choices for permitted business purposes with incompatible purposes.



- **Easy to execute.**

- Clicking “Do Not Sell or Share My Personal Information” should take consumers to the mechanism to exercise rights and must not require a consumer to scroll through the entire policy.

- **Standard-Forcing** – The Colorado Privacy Act Rule 7.09(E)

- “The fact that a design or practice is commonly used is not, alone, enough to demonstrate that any particular design or practice is not a Dark Pattern.”

Dark Patterns: Key Takeaways

- ✓ Review methods of consent and choice architecture against FTC and state guidelines.
- ✓ Choice buttons should be the same size and color.
- ✓ Pay attention to consumer complaints, as these will often initiate investigations or enforcement actions. If possible, conduct consumer testing (e.g., FTC Epic Games Case).
- ✓ Avoid product or service “rankings” that give the impression of objective or unbiased reviews, especially where rankings are based on third-party compensation.
- ✓ Watch out for a false sense of urgency.
- ✓ Disclose any unavoidable, mandatory fees in the upfront, advertised

price.



Thank You!

Questions & Contact Information

Reed Freeman

Reed.Freeman@afslaw.com

Michelle Bowling

Michelle.Bowling@afslaw.com