Generative Artificial Intelligence, Automated User Interfaces, and the New Laws of Dark Patterns

JUNE 29, 2023

D. REED FREEMAN JR.

Companies around the world are rushing to integrate generative artificial intelligence (GenAI) into their user interfaces to automate and deliver tailored website and application interfaces, customer service interactions, and advertising content to individual users in more personalized ways than ever.

But with the increased ease and effectiveness of automation, companies should now take care that the results of these efforts do not trigger a relatively new, and quickly growing set of "dark patterns" laws, regulations, and enforcement standards at the federal and state levels.

There is no way to implement a human review of all AI outputs, especially when they are generated at scale, but with a July 1 enforcement deadline for new laws in California, Colorado, and Connecticut quickly approaching, and with FTC enforcement already active, companies can, and should: (1) check representative samples of these outputs for compliance against emerging legal standards; (2) closely monitor consumer complaints; and (3) use the learnings from these activities to continue training their AI algorithms to avoid the creation of dark patterns in their user interfaces and choice architecture going forward.

This is an area of significant regulatory interest. The upside of compliance is not just a reduced regulatory risk profile, but also a competitive advantage in the use of AI to improve consumers' experiences and engagement. Failing to take action now could lead to costly and distracting investigations and negative press. It could also lead to disgorgement of not just the AI-generated output and data collected from it, but also the algorithms themselves,[1] which could set your company well behind your competitors in one of the fastest developing markets in generations.

What is a Dark Pattern?

The phrase "dark pattern" has been in the lexicon since 2010, when a user experience designer registered **darkpatterns.org** for the purpose of drawing attention to user interfaces that trick or manipulate consumers into making choices they would otherwise not have made and that cause harm.[2] Policymakers have since coalesced on a definition of "dark pattern" as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice."[3]

Dark Patterns – Emerging Rules

The Colorado Attorney General, the California Privacy Protection Agency (CPPA), and the Federal Trade Commission (FTC) have provided the detail on factors that they will consider in finding a user interface or choice architecture constitutes a dark pattern.

Colorado Privacy Act Rules

The Colorado Privacy Act (CPA) Rules have three-and-a-half pages on dark patterns in the context of consumer choice presentations, with six general rules and 30 sub-parts Rule 7.09 provides details on what user interface design characteristics will be considered in the context of choice presentation:

1. Choices must be displayed symmetrically. This includes size, font, coloring, and number of steps. Examples of common online displays that are now under scrutiny include presenting an "I do not accept" button in a greyed-out color while the "I accept" button is presented in a bright or obvious color and displaying an "I accept" button next to a "Learn More" button, which requires consumers to take an extra step before they are given the option of an "I do not accept" button.
2. No emotionally manipulative language. No guilt or shame in choice presentation. No unnecessary or gratuitous information to emotionally manipulate consumers. The line between sales and emotional manipulation is thin, so watch this area closely.
3. No interruptions. Consumers should not be redirected away from the content or service they are attempting to interact with because they declined the consent choice offered.
4. No false sense of urgency. This includes commonly used countdown clocks and limited inventory displays unless they are strictly accurate.
5. No double negatives, no confusing or unexpected syntax.
6. Consider the vulnerabilities of a product, service, or website when deciding how to present consent choice options.
7. Available through digital accessibility tools.

Rule 7.09 goes on to say this this list is not exhaustive and that controller may consider (meaning the state may enforce) other statutes, administrative rules, and administrative guidance concerning dark patterns from other jurisdictions when evaluating the appropriateness of the user interface or choice architecture used to obtain required consent. At a time when the market demands certainty, Colorado's rule is open-ended, essentially putting the entirety of discretion in the hands of the Attorney General based on what amounts to a subjective standard.

California CPRA Rules

Similarly, the California Privacy Rights Act (CPRA) amends the California Consumer Privacy Act (CCPA) Regulations to define dark patterns as a "user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice, as further defined by regulation."

Many of the user interface design characteristics described in the CCPA Regulations resemble the CPA's rules. Section 7004 of the CCPA Regulations lists design requirements businesses must follow for submitting CCPA requests and obtaining consumer consent, including:

1. Language used in disclosures and communications must be easily understood by consumers. Plain language is preferrable, and technical or legal jargon should be avoided.
2. No design elements that impair or interfere with a consumer's ability to make a choice. Consumers should not have to click through disruptive screens to submit an opt-out request. Choices should not be bundled together where the consumer is only offered one choice.
3. Easy execution of CCPA requests. Business should not add any unnecessary burdens or friction to the CCPA request process, such as additional steps to submit an opt-out request. Businesses that do not fix broken links, list non-functional email addresses, or require consumers to unnecessarily wait on a webpage while waiting on a request may be violating CCPA regulations.

Federal Trade Commission Guidance

The FTC has also provided guidance on what constitutes a dark pattern. It overlaps with Colorado and California regarding false senses of urgency and on designing for vulnerable populations, where appropriate.[4] Additionally, the FTC takes issue with:

1. Design elements that induce false beliefs, such presenting an interface that appears unbiased — a news article or a product comparison — when it is not unbiased.
2. Design elements that hide or delay the disclosure of material information, such as failing to display, or to display adequately, the full price, including fees.
3. Unintended or unauthorized purchases and subscription enrollments, such as in-app purchases by children without accountholder approval or unintended paid subscriptions or memberships.
4. Making it difficult to cancel a service or membership.
5. Placing material terms in a general terms and conditions document or behind hyperlinks, pop-ups, or dropdown menus.
6. Presenting toggle settings leading consumers to make unintended privacy choices, highlighting a choice that results in more information collection, and using default settings that maximize data collection and sharing.
7. Failing to clearly explain choices offered to consumers.

According to the FTC, "businesses should … assess their user interfaces from a consumer's perspective and consider whether another option might increase the likelihood that a consumer's choice will be respected and implemented."[5]

Regulatory Enforcement Actions Alleging Dark Patterns

While we wait for new state enforcement to come online after July 1, the FTC has been active in this area.

For example, the FTC recently brought an enforcement action against a marketing company for allegedly using dark patterns to trick consumers into falsely believing that purchases were necessary to enter a sweepstakes or would increase their chances of winning. The FTC alleged that the company's disclosures in small, light font, below "call to action" buttons, were inadequate. Among other things, the agreed order settling the matter requires the company to pay millions of dollars in equitable relief.

In another enforcement action, the FTC alleged that a gaming company designed confusing and counterintuitive button configurations within the game that made it easy for children to make unauthorized in-game purchases. The FTC alleged that children were also able to easily make in-app purchase without parental authorization, and that the company ignored complaints about this from consumers and even its own employees. The agreed order required the company to pay hundreds of millions of dollars in equitable relief.

The FTC also brought an enforcement action against a connected TV manufacturer, alleging that the company did not adequately disclose its default setting that automatically collected and shared consumers television viewing activity with third parties. The company settled the matter and agreed to pay millions of dollars in equitable relief.

How will regulators apply these rules? The FTC enforcement actions, as well as regulations the California and Colorado regulations, bring more clarity.

- Intent matters. A company's intent in designing the interface is a factor to be considered.
- Knowledge matters. If a business did not intend to design the user interface to subvert or impair user choice, but the business knows of this, through its customer complaints or otherwise, and does not remedy a user interface with that result, the user interface may be a dark pattern.
- Companies must take steps to monitor their user interfaces. A business deliberately ignoring the effects of its user interface may weigh in favor of establishing a dark pattern.[6] The FTC adds that if a business becomes aware that a particular design choice manipulates consumer behavior, the company should remediate the problem.
- Benchmarking practices against competitors is no defense. The fact that a design or practice is commonly used is not enough to demonstrate that any particular design or practice is not a dark pattern.[7]

Managing the Use of Generative AI to Create Compelling User Interfaces

1. Check representative samples for compliance against emerging legal standards.

Automated user interfaces can proliferate at scale. How do you ensure that the interface meets these regulatory standards? That it makes appropriate disclosures, is not emotionally manipulative, is capable of being understood by vulnerable populations? Displays choice architecture symmetrically? Or displays toggle settings consistent with users' expectations?

It's not possible, or at least efficient, to review each user interface and each set of choice architecture resulting from the use of automated GenAI. But companies can implement a human review of a sample that should meet statistical significance standards if done at regular intervals.

Reviews should look for the types of things that regulators are flagging as potential dark patterns in user interfaces and choice architectures. Because reviews may reveal sensitive information, they should be conducted under privilege. However, the types of changes that that are identified in these reviews should be identified and cataloged.

2. Monitor complaints, refund requests, and cancellations for spikes and trends.

Keep track of users' complaints, refund requests, and cancellations. Are consumers complaining about choices or purchases they did not intend? See if you can you identify the types of user interfaces or choice architectures that generate this activity. Identifying these things early allows you an opportunity to address them. It will also provide important inputs to help train your algorithms to avoid these issues going forward. Regulators receive only a small fraction of the complaints that companies get directly from consumers, and generally get them after companies do. Ending negative trends and flattening negative spikes is the easiest and most effective way to steer clear of regulatory trouble.

The FTC's enforcement action against Epic Games is illustrative. The FTC alleged that despite receiving more than one million complaints from consumers related to unwanted charges, Epic Games continued to charge users for in-game items without their authorization, and only made changes after it was already under FTC investigation. The FTC's reaction? A settlement for almost a quarter-billion dollars.

3. Use the amended outputs to continue training AI algorithms used to train your algorithms going forward.

After reviewing consumer correspondence and complaints, and the types of issues identified in your review of samples of user interfaces and choice architectures, you're ready for the next step. Discuss your findings, under privilege, with business and engineering teams and drive toward feeding these learnings into your algorithms. That way, your user interfaces and choice architectures will improve over time, allowing you to continue to tailor them to be more engaging for users with a decreasing risk profile.

Conclusion

GenAI offers extraordinary promise for providing more personalized user experiences than ever before. Policymakers, however, have made clear — in legislation, regulation, and enforcement actions — that this technology could manipulate users' autonomy and decisionmaking.

The July 1 enforcement date for the CPRA and the Colorado Privacy Act – each of which addressed dark patterns, is fast approaching. And the FTC is already enforcing its dark patterns theory of liability aggressively. Now is the time to implement a process to review samples of your user interfaces and consumers' complaints and correspondence. Take care – under privilege – to catalog issues for remediation, and then work with business and engineering teams to feed those learnings into your user interface algorithms. By taking these steps, you will continue to enjoy the fruits of your technology while at the same time reducing your risk profile in the new and expanding age of dark patterns policy and enforcement.

Additional research and writing from Natalie Tantisirirat, a 2023 summer associate in ArentFox Schiff's San Francisco office and a law student at University of California College of the Law, San Francisco.

---

[1] See In the **Matter of Everalbum** (May 2021)(Order).

[2] See **FTC Staff Report**, Bringing Dark Patterns to Light (2022) at p. 2.

[3] See California: **Cal. Civ. Code 1798.140(l)**,

Colorado: **Colorado Privacy Act, C.R.S. § 6-1-1303(9)**,

Connecticut: **Personal Data Privacy and Online Monitoring Act, § 1(11)**. See also FTC Staff Report, Bringing Dark Patterns to Light (2022) at p. 2.

[4] See FTC Staff Report, Bringing Dark Patterns to Light at pp. 4, 9.

[5] Id. at 18.

[6] **California Consumer Privacy Act Regulations § 7004(c)**.

[7] **Colorado Privacy Act Rule 7.09(E)**.

Contacts

D. Reed Freeman Jr.

PARTNER

Related Practices

Privacy, Data Protection & Data Security

Continue Reading

ALERTS

Employers Take Note: EEOC Begins Enforcing The Pregnant Workers Fairness Act

JUNE 29, 2023 | HENRY MORRIS, JR.

ALERTS

Illinois Supreme Court Adopts Partial Breach Doctrine

JUNE 28, 2023 | JIN YAN

ALERTS

Midyear Update on PBM Reform

JUNE 26, 2023 | SARAH B. “CISSY” JACKSON, DANIEL SJOSTEDT*

All Perspectives from Alerts