



Dark Patterns: Manipulative Digital Design

NAIC Market Regulation and Consumer Affairs (D) Committee

August 12, 2022

Birny Birnbaum
Center for Economic Justice

The Center for Economic Justice

CEJ is a non-profit consumer advocacy organization dedicated to representing the interests of low-income and minority consumers as a class on economic justice issues. Most of our work is before administrative agencies on insurance, financial services and utility issues.

On the Web: www.cej-online.org

About Birny Birnbaum

Birny Birnbaum is the Director of the Center for Economic Justice, a non-profit organization whose mission is to advocate on behalf of low-income consumers on issues of availability, affordability, accessibility of basic goods and services, such as utilities, credit and insurance.

Birny, an economist and former insurance regulator, has worked on racial justice issues for 30 years. He has been involved with and studied insurance consumer disclosures for over 30 years as a regulator, consultant and consumer representative. He has served for many years as a designated Consumer Representative at the National Association of Insurance Commissioners and is a member of the U.S. Department of Treasury's Federal Advisory Committee on Insurance, where he co-chairs the subcommittee on insurance availability.

Birny served as Associate Commissioner for Policy and Research and the Chief Economist at the Texas Department of Insurance. Prior to TDI, Birny was the Chief Economist at the Texas Office of Public Insurance Counsel, a state agency dedicated to representing consumers before the TDI.

Birny was educated at Bowdoin College and the Massachusetts Institute of Technology. He holds Master's Degrees from MIT in Management and in Urban Planning with concentrations in finance and applied economics. He holds the AMCM certification.

Why CEJ Works on Insurance Issues

Insurance Products Are Financial Security Tools Essential for Individual and Community Economic Development:

CEJ works to ensure ***fair access*** and ***fair treatment*** for insurance consumers, particularly for low- and moderate-income consumers.

Insurance is the Primary Institution to Promote Loss Prevention and Mitigation, Resiliency and Sustainability:

CEJ works to ensure insurance institutions maximize their role in efforts to reduce loss of life and property from catastrophic events and to ***promote resiliency and sustainability*** of individuals, businesses and communities.

What is a Dark Pattern?

“Dark patterns are user interface techniques that benefit an online service by leading consumers into making decisions they might not otherwise make. Some dark patterns deceive consumers, while others exploit cognitive biases or shortcuts to manipulate or coerce them into choices that are not in their best interests.”

As documented in several research studies, consumers may encounter dark patterns in many online contexts, such as when making choices to consent to the disclosure of personal information or to cookies, when interacting with services and applications like games or content feeds that seek to capture and extend consumer attention and time spent, and in e-commerce, including at multiple points along a purchasing journey.

Source: <https://freedom-to-tinker.com/2022/08/10/recommendations-for-updating-the-ftcs-disclosure-guidelines-to-combat-dark-patterns/>

“At their core, dark patterns are a specific type of choice architecture in website and app design that interfere with user autonomy and choice. Dark patterns modify the presentation of choices available to users or manipulate the flow of information so that users make selections that they would not otherwise have chosen—to their own detriment and to the benefit of the website or app provider. [Hallmarks](#) of dark patterns include imposing asymmetric burdens to achieve competing choices, restricting the choices available at the same time (or at all), and hiding information or presenting information deceptively.”

“Dark patterns can exist when one option is more aesthetically prominent or attractive, or when the alternative is hidden or arduous to select. For example, a website may offer a popup with only a “yes” button, but leave out a “no” button and/or require more clicks to achieve the “no” option. Or, a button may have undesired consequences, as when closing a popup banner functions as acceptance rather than rejection.”

Source: <https://www.bytebacklaw.com/2022/03/how-do-the-cpra-cpa-and-vcdpa-treat-dark-patterns/>

Dark User Experience is Different from Bad User Experience

Bad UX is accidental. It is a bad design from a lack of knowledge in design. Whereas, dark UX is intentional and purposely designed to promote the brand's best interests at the user's expense.

- Bad UX: Confusing checkout processes.
- Dark UX: Purposefully making it difficult to find “x” that closes a pop-up.

Brands that use dark UX know exactly what they're doing. They are well aware of the UX concepts that make websites great and use that knowledge to manipulate their users.

Source: <https://medium.com/galaxy-ux-studio/how-do-dark-ux-patterns-affect-users-e74a4496c06e>

What are Examples of Dark Patterns Techniques?

From Jamie Liguri published in “Shining a Light on Dark Patterns.”

Nagging: Repeated requests to do something the firm prefers

Confirmshaming: Choice framed in a way that makes it seem dishonorable or stupid.

Forced Action: Requiring opt-out of optional services, manipulative extraction of personal information and information about other users

Social Proof: False/misleading notices that others are purchasing or offering testimonials

Roach Motel: Asymmetry between signing up and canceling

Price Comparison Prevention: Difficult in understanding and comparing prices

Hidden Information / Aesthetic Manipulation: Important information visually obscured

From the European Consumer Organization, “Fast Track to Surveillance”
<https://www.beuc.eu/fast-track-surveillance>

“During this signup process, which involves consumers taking important decisions about how Google will process their personal data, the tech giant uses a combination of deceptive design, unclear language, misleading choices and missing information:

- With only one step (“express personalisation”), the consumer activates all the account settings that feed Google’s surveillance activities. Google does not provide consumers with the option to turn all settings ‘off’ in one step.
- If consumers want to try to protect their privacy, it requires “manual personalisation”: five steps with ten clicks and grappling with information that is unclear, incomplete, and misleading

Consider the consent for use of cookies on most websites. In almost every case, one click is required to accept all cookies. If you want to avoid sharing your personal information, it requires many clicks.

How Effective are Dark Patterns?

From Liguri and Strahilivetz Testing:

Condition	Acceptance Rate	Adjusted Acceptance Rate (treats drop-outs as declines)
Control Group	11%	11%
Mild Dark Pattern	26%	25%
Aggressive Dark Pattern	42%	37%

“Normative Take-aways” from Liguri and Strahilivetz

- The mild dark patterns are the most insidious. They significantly increased acceptance of a program with dubious benefits without alienating consumers or causing large numbers of them to log off
- Less educated subjects were particularly vulnerable to dark patterns
- Effects of dark patterns swamp effects of price changes
- Dark patterns vary substantially in terms of potency
- Dark patterns have proliferated because they work

Legislative and Regulatory Actions on Dark Patterns

- California Consumer Privacy Act
 - (l) “Dark pattern” means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice, as further defined by regulation.

And

Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent.

Source: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

- Colorado Privacy Act

- "DARK PATTERN" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice

Source: https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf#page=4

- Connecticut Personal Data Privacy Act

- "Dark pattern" (A) means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice, and (B) includes, but is not limited to, any practice the Federal Trade Commission refers to as a "dark pattern".

Source: <https://www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF#page=2>

- Federal Legislation: Senate Bill 1084 – Deceptive Experiences to Online Users Reduction Act
 - (1) IN GENERAL .—It shall be unlawful for any large online operator
 - (A) to design, modify, or manipulate a user interface with the purpose or substantial effect of obscuring, subverting, or impairing user autonomy, decision-making, or choice to obtain consent or user data;
 - (B) to subdivide or segment consumers of online services into groups for the purposes of behavioral or psychological experiments or studies, except with the informed consent of each user involved;

Source: <https://www.congress.gov/116/bills/s1084/BILLS-116s1084is.pdf>

Federal Trade Commission Enforcement Using Authority to Regulate “Unfair and Deceptive Practices.”

“The Federal Trade Commission issued a new [enforcement policy statement](#) warning companies against deploying illegal 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 cancel.

The FTC’s policy statement puts companies on notice that they will face legal action if their sign-up process fails to provide clear, up-front information, obtain consumers’ informed consent, and make cancellation easy.”

Source: <https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-ramp-enforcement-against-illegal-dark-patterns-trick-or-trap-consumers-subscriptions>

Consumer Financial Protection Bureau

“Today, the Consumer Financial Protection Bureau (CFPB) is filing a lawsuit against TransUnion, two of its subsidiaries, and longtime executive John Danaher for violating a 2017 law enforcement order. The order was issued to stop the company from engaging in deceptive marketing, regarding its credit scores and other credit-related products. After the order went into effect, TransUnion continued its unlawful behavior, disregarded the order’s requirements, and continued employing deceitful digital dark patterns to profit from customers.

Source; <https://www.consumerfinance.gov/about-us/newsroom/cfpb-charges-transunion-and-senior-executive-john-danaher-with-violating-law-enforcement-order/>

Critical for Regulators to Understand and Address Dark Patterns

- Insurance regulatory disclosures are based on and designed for paper, not digital interfaces. What does it mean to “prominently display” certain information or provide in a “10-point” font when the disclosure and consent are done on a computer or mobile phone?
- Paper disclosures are static. Digital disclosures are dynamic and change based on the particular consumer, the method of consumer interaction and the choices by the consumer during the process.
- There has been a massive and rapid increase in digital interactions in place of paper or face-to-face interactions between consumers and insurers. Consider digital claim settlements as well as interactions involving insurance application and receipt of policy and other information.

How Should Regulators, D Committee, NAIC Address Dark Patterns?

- Learn -- Train Analysts and Examiners to Recognize Dark Patterns and Manipulative Digital Design.
- Compile Resources on Manipulative Digital Design.
- Review Existing Disclosure Requirements – Do They Make Sense for a Digital Interface and Protect Against Dark Patterns?
- Update Guidance in Regulations as Needed – Not Just Revisions in Disclosures and Disclosure Requirements, but Articulating Dark Patterns as an Unfair and Deceptive Trade Practice.
- Develop Relevant Methods of Regulatory Review / Update the Market Regulation Handbook.

Additional Resources:

Liguri and Strahilivetz, “Shining a Light on Dark Patterns”

The Regulatory Review, “Dark Patterns Cannot Stay in the Dark”

<https://www.theregreview.org/2022/05/28/saturday-seminar-dark-patterns-cannot-stay-in-the-dark/>

Harry Brignull’s Deceptive Design Website: <https://www.deceptive.design/>

CHOICE (Australia), “Consumers being harmed by “dark patterns” in web design”

<https://www.choice.com.au/consumers-and-data/data-collection-and-use/how-your-data-is-used/articles/dark-patterns-cprc>

Squire, Patton Boggs LLP, “Dark Patterns are Focus of Regulatory Scrutiny in the United States and Europe”

<https://www.natlawreview.com/article/dark-patterns-are-focus-regulatory-scrutiny-united-states-and-europe>

European Data Protection Board, “Dark patterns in social media interfaces: How to recognize and avoid them”