



Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Via electronic filing (regulations.gov)

May 28, 2021

Re: Topics to be Discussed at Dark Patterns Workshop (Docket ID: FTC-2021-0019-0001)

Dear Federal Trade Commission:

Access Now¹ appreciates the opportunity to provide written comments following the Federal Trade Commission's (FTC's) workshop, *Bringing Dark Patterns to Light*. Below, we provide specific feedback to questions posed by the FTC. We look forward to working with the FTC and all stakeholders to address the concerns raised in our comments. We aim to advance essential policy changes and enforcement practices necessary to ensure consumers can adequately and autonomously exercise their privacy rights in the digital world.

Introduction

Many people looking to connect with family and friends, engage in commerce, and educate and entertain themselves online will encounter dark patterns. They have infiltrated practically every marketing and sales business model online including shopping websites, social media, mobile and video games, and mobile applications.

While defying any single definition, one can understand a dark pattern as a user interface design choice in a product or service that attempts to influence a person's decision, often toward a decision that is against the person's best interests and in favor of the provider's interest.² These designs may draw attention to, or reduce attention to, particular options, statements, or other aspects of the service. Much effort has gone into defining and identifying various types of dark patterns and creating taxonomies and tracking examples.³ While some highlight the characteristics of particular dark

¹ Access Now is an international organization that defends and extends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for a free and open internet that fosters human rights. As part of our mission, we operate a global digital security helpline for users at risk to mitigate specific threats they face. Additionally, we work directly with lawmakers at national and international fora to ensure policy decisions are focused on the rights and interests of users, particularly those most at risk. See <https://www.accessnow.org>.

² The original definition from Harry Brignull is "Dark Patterns are tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up for something." DarkPatterns.org, <https://www.darkpatterns.org>.

³ Arunesh Mathur, *et al.*, *What Makes a Dark Pattern... Dark?*, CHI Conference on Human Factors in Computing Systems (CHI '21) (May 8–13, 2021), <https://arxiv.org/pdf/2101.04843.pdf>.

patterns, others describe how dark patterns influence users.⁴ Both are equally important concepts but a one-size-fits-all definition eludes us.

Rather than focus on a definition of dark patterns upfront, we focus on people's perspectives and harms resulting from specific dark patterns. Whether it is a loss of agency, privacy, money, or time, dark patterns make it very difficult for users, or even deny users the ability, to make autonomous and informed decisions. Such designs do not build loyalty or trust, instead they often leave consumers feeling tricked or shamed.

Crafting a regime that ensures the FTC can hold companies accountable for using dark patterns to induce actions that are not in people's best interest is essential to protect people from the harms that result. Companies should design their products and services with and for their most vulnerable users. This principle means, at a minimum, providing easy-to-understand and transparent interface designs that preserve user autonomy and agency. The FTC should hold those companies that do not design their products in such a way accountable.

In these comments, we highlight several issues regarding the ability of dark patterns to influence decision making, and behavior. We highlight many of the reported harms that deserve careful examination and refinement before precise policy action is considered. We first explain the effectiveness of dark patterns, then we discuss how they influence people into giving up their private information, autonomy, money, and time, and last we discuss how the FTC should use its unfairness authority to protect against dark patterns.

Companies use dark patterns to influence people into making undesirable decisions, causing them harm.

Companies have increasingly been employing dark patterns to influence individual choice online.⁵ There are several types of dark patterns that companies use, far too many to list here. However, some are worth pointing out. "Confirmshaming" is a popular dark pattern where a company will attempt to guilt a user into choosing the option that best suits the company. Suppose a person wants to remove themselves from a commercial email subscription. Some companies make the process simple, including a direct link that when clicked, automatically removes the individual from the list. Other companies employ various tools to keep a person on their lists. They might tell a person that if they unsubscribe, they would miss out on important deals or offers, an example of confirmshaming.

⁴ *Id.*; Daniel Susser, *et al.*, *Online Manipulation: Hidden Influences in a Digital World*, 4.1 Geo. L. Tech. Rev. 1 (2019), <https://philarchive.org/archive/SUSOMHv1>; Chris Baraniuk, *How 'Dark Patterns' Influence Travel Bookings*, BBC (Dec. 12, 2019),

<https://www.bbc.com/worklife/article/20191211-the-fantasy-numbers-that-make-you-buy-things-online>.

⁵ Sara Morrison, *Dark Patterns, the Tricks Websites Use to Make You Say Yes, Explained*, Vox Recode (Apr. 1, 2021), <https://www.vox.com/recode/22351108/dark-patterns-ui-web-design-privacy>; Arunesh Mathur, *et al.*, *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, Cornell University (Sept. 20, 2019), <https://arxiv.org/pdf/1907.07032.pdf>; Carol Moser, *et al.*, *Impulse Buying: Design Practices and Consumer Needs*, CHI '19: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems Paper No.: 242 at 1–15 (May 2019), <https://doi.org/10.1145/3290605.3300472>; Colin Gray, *et al.*, *The Dark (Patterns) Side of UX Design*, CHI '18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (April 2018), <https://doi.org/10.1145/3173574.3174108>.

Another example is when a person attempts to decline Amazon Prime, the company characterizes the choice as “No thanks, I don’t want Unlimited One-Day Delivery.”⁶

In other instances, companies use highly confusing “trick question” prompts that make it difficult for the person to achieve their desired outcome.⁷ Trick questions are most often seen in websites that introduce “confusing double negatives (e.g., ‘Uncheck the box if you prefer not to receive email updates’), or by using negatives to alter expected courses of action, such as checking a box to opt out (e.g., ‘We would like to send you emails. If you do not wish to be contacted via email, please ensure that the box is not checked’).”⁸ These dark patterns trick users by influencing their “decision in a way that may not be advantageous to their needs by using words, user experience or user interface elements to persuade the user in an unintended direction.”⁹

“Bait and switch” is another dark pattern that occurs when a person is shopping for a “good or service that was advertised but is then shown a barrage of ads for things the customer does not want.”¹⁰ One egregious example of this is when Microsoft pushed a Windows update, if a user clicked the “X” in the upper-right corner of the window, likely attempting to close the window without updating, it instead agreed to install the update.¹¹ Another example occurred when ProPublica in April 2019 uncovered a TurboTax dark pattern where the company advertised a “Free Guaranteed” service for lower-income taxpayers. However, when ProPublica staged a profile of a “house cleaner and cashier” who made less than \$66,000 to sign up for the product, they were led to paid products and found the path to the free version very difficult to find.¹²

Dark patterns can lead people to over-share personal information, potentially leading to harms like privacy breaches or embarrassment. “Privacy zuckering,”¹³ named after Facebook’s CEO, is when an online platform tricks someone into publicly sharing more information about themselves than they intended.¹⁴ Today, it takes place mainly behind the scenes.

Here's how it works: when you use a service (e.g. a store card), the small print hidden in the Terms and Conditions gives them permission to sell your personal data to anyone. Data brokers buy it and combine it with everything else they find about you online into a profile, which they then resell. Your profile may contain information

⁶ Confirmshaming, DarkPatterns.org, <https://www.darkpatterns.org/types-of-dark-pattern/confirmshaming>.

⁷ Harry Brignull, *Dark Patterns: Inside the Interfaces Designed to Trick You*, Verge (Aug. 29, 2013), <https://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you>.

⁸ Mathur, *Dark Patterns at Scale*, at 17.

⁹ Felt Tricked, Dark Patterns Tip Line, <https://darkpatternstipline.org/harms/felt-tricked>. For more on the Dark Patterns Tip Line, go to <https://darkpatternstipline.org>.

¹⁰ Jamie Luguri & Lior Strahilevitz, *Shining a Light on Dark Patterns*, University of Chicago Public Law Working Paper No. 719, at 50 (Mar. 29, 2021), <http://dx.doi.org/10.2139/ssrn.3431205>; see also Bait and Switch, DarkPatterns.org, <https://www.darkpatterns.org/types-of-dark-pattern/bait-and-switch>.

¹¹ Bait and Switch, DarkPatterns.org, <https://www.darkpatterns.org/types-of-dark-pattern/bait-and-switch>.

¹² Lucas Waldron & Justin Elliott, *Here's How TurboTax Just Tricked You Into Paying to File Your Taxes*, ProPublica (Apr. 22, 2019), <https://www.propublica.org/article/turbotax-just-tricked-you-into-paying-to-file-your-taxes>.

¹³ Privacy Zuckering, DarkPatterns.Org, <https://www.darkpatterns.org/types-of-dark-pattern/privacy-zuckering>.

¹⁴ Arielle Pardis, *How Facebook and Other Sites Manipulate Your Privacy Choices*, Wired (Aug. 12, 2020), <https://www.wired.com/story/facebook-social-media-privacy-dark-patterns>.

about your sexual preferences, physical and mental health. In theory your profile could result in you being refused services such as insurance or loans.¹⁵

These and other dark patterns cause harm. As discussed below, dark patterns can cost people money by influencing people to purchase products or services they would not normally want.¹⁶ Websites, particularly shopping and travel sites, use various dark patterns to push people into spending more money than they planned.¹⁷ They also cost people time by forcing people to click through several menus or pages that are unnecessary, called “nagging.”¹⁸ And people may simply feel a sense of shame, embarrassment, or frustration having either been duped by a dark pattern or made powerless to change their decision.¹⁹

Dark patterns can “affect people's emotions and behavioral patterns on a deep level, and it is uncertain how aware the common user is of these underlying design patterns, given their recent development and uptake.”²⁰ For example, confirmshaming statements may have a material effect on depressed individuals predisposed to experiencing a debilitating lack of motivation. When a depressed individual encounters confirmshaming tactics online, they may be more likely to choose the positively-framed option.²¹ On the other hand, for people prone to panic and anxiety disorders experiencing high levels of panic and confusion, confirmshaming can make it almost impossible to select what they first desired.²²

Dark Patterns are effective at influencing consumer choice, decision-making, and behavior, even when they are mild.

Dark patterns are generally most effective when the design is incredibly demanding on the person. It is important to note, however, that even minor dark patterns, which apply comparatively less pressure to a person to influence their decision, including by only changing the color of one option or highlighting some words, can affect individual choice. For instance, researchers in a recent study engaged a set of respondents in a privacy survey that ultimately identified all participants as privacy-conscious.²³ The researchers then told the respondents that they were going to be signed up for a subscription for an identity theft service, unless they refused at that point. The study split the respondents into three groups: the control (no dark patterns), the mild dark pattern, and the aggressive dark pattern.

¹⁵ Privacy zuckering, *supra* note 13.

¹⁶ Sidney Fussell, *The Endless, Invisible Persuasion Tactics of the Internet*, Atlantic (Aug. 5, 2019), <https://www.theatlantic.com/technology/archive/2019/08/how-dark-patterns-online-manipulate-shoppers/595360>.

¹⁷ Mathur, *supra* note 3, at 13.

¹⁸ *Id.* at 6.

¹⁹ Priya Singh, *Dark Patterns and How It Affects the Elderly*, Medium (May 7, 2020), <https://medium.com/students-nidblr/dark-patterns-and-how-it-affects-the-elderly-b9389102d62>; *see also* Felt Shamed, Dark Patterns Tip Line, <https://darkpatternstipline.org/harms/felt-shamed>.

²⁰ Maximilian Maier, *Dark Patterns – An End User Perspective*, Umeå University (2019), <http://urn.kb.se/resolve?urn=urn:nbn:se:umu:diva-160937>.

²¹ Ashley Firth, *How Dark Patterns on the Web Affect Your Mental Health*, mrfirthy.me (July 22, 2020), <https://mrfirthy.me/blog/how-dark-patterns-affect-mental-health>.

²² *Id.*

²³ Luguri, *Shining a Light on Dark Patterns*.

The mild dark pattern included false hierarchy by suggesting that accepting the identity theft coverage was “recommended,” and it also included confirmshaming by requiring the person to click on the option that said “I do not want to protect my data or credit history.”²⁴ Those declining coverage were then asked to explain why, with several pre-formed options like “Even though 16.7 million Americans were victimized by identity theft last year, I do not believe it could happen to me or my family,” and “I’ve got nothing to hide so if hackers gain access to my data I won’t be harmed.”²⁵ And of course, there was an easy option to sign up for the service on that page.

In the aggressive dark pattern condition, participants attempting to decline the identity theft protection faced even more significant hurdles. Those who declined were forced to read more information about identity theft, and forced to wait at least ten seconds before moving onto the next page, where they encountered a countdown timer. Participants that declined again were taken to another page with another countdown timer. There was then a third screen for those declining, with the same dark patterns, making this a nagging dark pattern. Those sticking out the process and declining the whole way were presented with the following trick question:

If you decline this free service, our corporate partner won’t be able to help you protect your data. You will not receive identity theft protection, and you could become one of the millions of Americans who were victimized by identity theft last year. Are you sure you want to decline this free identity theft protection?²⁶

Participants had two options: “No, cancel” and “Yes.” What each option does is unclear, and the correct answer to decline the service was actually “Yes.” If they guessed the correct answer, they were then taken to a page asking them to indicate their reason for declining the program.²⁷

The results were striking. Only 11.3% of respondents in the control accepted the service. In the mild group, the rate more than doubled to 25.8%. In the aggressive group, the rate increased to 41.9%.²⁸ Clearly there is evidence that “dark patterns effectively bend consumers’ will.”²⁹ Further, the dark patterns in this study were used in an attempt to convince people to spend money, something we typically assume garners a heightened sense of attention and care. The effectiveness of dark patterns in areas where money is not involved is likely even higher, as people have been known to give away their personal information even when warned about the dangers of doing so.³⁰

Dark patterns are especially effective against those without a college education and the elderly. These populations may lack the skills, knowledge, or ability to understand how these practices work.³¹ In

²⁴ *Id.* at 61-62.

²⁵ *Id.* at 62.

²⁶ *Id.* at 63.

²⁷ *Id.*

²⁸ *Id.* at 64.

²⁹ *Id.*

³⁰ Marianne Junger, *et al.*, *Priming and Warnings Are Not Effective to Prevent Social Engineering Attacks*, 66 *Computers in Human Behavior* 75, 83 (2017), <http://jandmparker.net/research/Priming%20and%20warnings%20are%20not%20effective%20to%20prevent%20social%20engineering.pdf>.

³¹ Singh, *supra* note 19.

particular, certain aspects of dark patterns are confusing for older adults, including that they do not understand the difference between multiple, similar-looking buttons, and they perceive green and blue buttons as “correct” and red and orange buttons as “dangerous.”³² The lack of digital literacy among less-educated groups may also be the reason dark patterns work effectively against users without a college education. In one study, less-educated subjects were significantly more susceptible to mild dark patterns.³³

Game developers are using dark patterns to keep gamers gaming.

Dark patterns have infiltrated the gaming industry as well, where companies use dark patterns to influence user behavior and achieve their objectives, generally getting people to spend more money. Gaming is a significant business, with 2021’s global games market expected to generate revenues of \$175.8 billion.³⁴ Dark patterns likely play a role in why the industry is so lucrative..

Dark patterns found in game designs are, by one definition, “used intentionally by a game creator to cause negative experiences for players which are against their best interests and likely to happen without their consent.”³⁵ Gaming dark patterns can also cause gamers to waste time and money, particularly around loot boxes.³⁶ For example, dark patterns used by game developers include the “Pay to Skip” technique, “where a developer charges users to solve in-game challenges and creates an uneven playing field for paying and non-paying users.”³⁷ Pay to skip is often used in conjunction with “grinding,” which is uninteresting, repetitive aspects of games where players will be more likely to pay to avoid the inconvenience of grinding.³⁸ Another example is in *Plants vs. Zombies 2*, gamers have the option of paying coins to retry a failed event.³⁹

In the gaming context, this type of emotional and psychological deception can cause players to become addicts. Researchers in *Dark Patterns in Player Experience for Kids: The Case of Fortnite*, explored dark patterns in game design and their impact on players. People have reported 371 dark patterns that wasted their time, and 310 dark patterns that wasted their money.⁴⁰ The list is extensive, but to name just a few, some of the dark patterns found in the game included the Pay to Skip design, allowing gamers to pay money to avoid waiting for a timer to expire, and the “Premium Currency” design which disguises the real price of items when players exchange between real money and

³² *Id.*

³³ Luguri, *supra* note 10.

³⁴ Tom Wijman, *Global Games Market to Generate \$175.8 Billion in 2021*, NewZoo (May 6, 2021), <https://newzoo.com/insights/articles/global-games-market-to-generate-175-8-billion-in-2021-despite-a-slight-decline-the-market-is-on-track-to-surpass-200-billion-in-2023>.

³⁵ Jose P. Zagal, *et al.*, *Dark Patterns in the Design of Games*, Foundations of Digital Games Conference (May 14-17, 2013), at 3, http://www.fdg2013.org/program/papers/paper06_zagal_et_al.pdf.

³⁶ Scott A. Goodstein, *When the Cat’s Away: Techlash, Loot Boxes, and Regulating “Dark Patterns” in the Video Game Industry’s Monetization Strategies*, University of Colorado Law Review (Feb 1, 2021), <https://lawreview.colorado.edu/printed/when-the-cats-away-techlash-loot-boxes-and-regulating-dark-patterns-in-the-video-game-industrys-monetization-strategies>.

³⁷ Mathur, *supra* note 3 at 6.

³⁸ Grinding, DarkPattern.games, <https://www.darkpattern.games/pattern/12/grinding.html>.

³⁹ Pay to Skip, <https://www.darkpattern.games/pattern/34/pay-to-skip.html>.

⁴⁰ Fortnite Dark Patterns, DarkPattern.Games, <https://www.darkpattern.games/game/29/0/fortnite.html>.

in-game currency.⁴¹ The impact on gamers ranged from a change in mood to decreased or no outdoor activity, isolation, and even in some cases, “little” robberies.⁴²

The FTC should take action against companies that use dark patterns, which can be unfair.

Unfair practices can result in significant financial injury to people, erode consumer confidence, and undermine the financial marketplace. Dark patterns can be at least an unfair practice.

Section 5 of the FTC Act prohibits, in part, “unfair ... acts or practices in or affecting commerce.”⁴³ A practice is unfair if it causes injury to consumers that is substantial, without offsetting benefits, and not reasonably avoidable.⁴⁴ “Substantial injury” includes small harms inflicted on a large number of people.⁴⁵ “Reasonably avoidable” focuses on whether there was an “obstacle to the free exercise of consumer decision-making.”⁴⁶

Dark patterns can be unfair. For the reasons above, dark patterns cause harm to people. They influence people to make decisions not in their favor, ranging from continuing to subscribe to a service to giving up more information than is necessary. Even if that were not enough, societal harms suffice for substantial injury, and should be sufficient here. There are similarly no offsetting benefits to dark patterns. If anything, dark patterns trap people into a service when they would prefer to use the services of another (or no one), a result that limits competition and benefits no one but the purveyor of the dark pattern. Dark patterns are often not avoidable, particularly those that seek to prevent a person from canceling a subscription, or dark patterns that induce a person to give up more information than they need to (those people may not even know they have the option not to provide the information). People often will not know when and where dark patterns exist on a certain service or product, as there are no labels or warnings. Dark patterns are surprises and may even be unknown to the person who is the unwitting subject of one.

Given the remarkably extensive use of dark patterns by major online platforms and app developers, perhaps the only way to curb their abuse would be for the FTC to stop companies from employing them using its Section 5 authority. The FTC should also consider encouraging or, where possible, requiring companies to audit their websites and apps for known dark patterns so they can be removed.

⁴¹ *Id.*

⁴² Rosa Gil & Carina González, *Dark Patterns in Player Experience for Kids: The Case of Fortnite*, CHI 2020 - ACM CHI Conference on Human Factors in Computing Systems (2020), https://www.researchgate.net/publication/339617770_Dark_patterns_in_player_experience_for_kids_the_case_of_Fortnite.

⁴³ 15 U.S.C. §45(a).

⁴⁴ J. Howard Beales, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, FTC Blog (May 30, 2003), <https://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection>.

⁴⁵ FTC Policy Statement on Unfairness, FTC (Dec. 17, 1980), <https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness>

⁴⁶ Beales, *supra* note 44 (citing FTC Policy Statement on Unfairness).

Conclusion

Dark patterns are a serious concern, as they can cause extensive harm to people, particularly vulnerable people. The FTC should investigate dark patterns, and use their Section 5 authority to take action against their use.

Respectfully submitted,

Willmary Escoto
U.S. Policy Analyst

Eric Null
U.S. Policy Manager

[Access Now](#)