

Bringing Dark Patterns to Light

STAFF REPORT | SEPTEMBER 2022

Introduction

For decades, unscrupulous direct mail marketers and brick-and-mortar retailers have relied on design tricks and psychological tactics, such as pre-checked boxes, hard-to-find-and-read disclosures, and confusing cancellation policies, to get consumers to part with their money or data. As more and more commerce has moved online, so too have these manipulative design practices—termed “dark patterns”—only they have grown in scale and sophistication, creating ever greater challenges for consumers.¹

As the nation’s leading consumer protection agency, the Federal Trade Commission’s (“FTC”) mission is to stop deceptive or unfair business practices in the marketplace, including those that take the form of dark patterns.² The FTC has, for example, sued companies for requiring users to navigate a maze of screens in order to cancel recurring subscriptions, using non-descript dropdown arrows or small icons to hide the full cost and other terms of rent-to-own or other payment products, and even sneaking unwanted products into consumers’ online shopping carts without their knowledge.³ More recently, the agency issued an enforcement policy statement that warned companies against deploying illegal practices that trick or trap consumers into subscription services.⁴

On April 29, 2021, the FTC hosted a public workshop on digital dark patterns and explored whether user interfaces can have the effect of obscuring, subverting, or impairing consumer autonomy and decision-making.⁵ The workshop featured a variety of speakers, including consumer advocates, members of Congress, researchers, legal experts, and other industry professionals. In this Staff Report, we discuss key topics from the workshop and academic literature, including the rise of dark patterns in the digital marketplace and common types of dark patterns. (See Appendix A.) For each common dark pattern addressed, we discuss consumer protection concerns and recommendations for companies.



Bringing **Dark Patterns** to **Light**

AN FTC WORKSHOP

Background

Coined in 2010 by user design specialist Harry Brignull, the term “dark patterns” has been used to describe design practices that trick or manipulate users into making choices they would not otherwise have made and that may cause harm.⁶ As the workshop’s panelists noted, dark patterns often take advantage of consumers’ cognitive biases to steer their conduct or delay access to information needed to make fully informed decisions.⁷ Research shows that dark patterns are highly effective at influencing consumer behavior. For example, one study discussed at the workshop found that dark patterns doubled the percentage of consumers who signed up for a dubious identity theft protection service, as compared to consumers who were presented with a neutral interface. And these effects increased significantly when test subjects were exposed to more than one dark pattern.⁸

...the term “dark patterns” has been used to describe design practices that trick or manipulate users into making choices they would not otherwise have made and that may cause harm.

Dark patterns often are not used in isolation and tend to have even stronger effects when they are combined.⁹ (See Appendix B.) Multiple examples from FTC enforcement matters bear this out. In *Raging Bull*, for instance, the FTC alleged that the operators of an online stock trading site used deceptive customer testimonials to lure consumers in, hid purported disclaimers in dense terms and conditions text boxes that required scrolling to find, and sold services as a subscription but made it difficult to cancel and stop the recurring charges.¹⁰ The combination of these dark patterns had a compounding effect, increasing the impact of each and exacerbating the harm to the consumer.

Panelists noted that the use of manipulative design techniques in the digital world can pose heightened risks to consumers.¹¹ The pervasive nature of data collection techniques, which allow companies to gather massive amounts of information about consumers’ identities and online behavior, enables businesses to adapt and leverage advertisements to target a particular demographic or even a particular consumer’s interests.¹² Moreover, companies that market online can experiment with digital dark patterns more easily, frequently, and at a much larger scale than traditional brick-and-mortar retailers, to determine which design features most effectively influence consumer behavior.¹³ (By contrast, consider the practical difficulties of incessantly rearranging the aisles of a grocery store that places sugary cereals at toddler eye-level and candy bars at the register to do the same.)¹⁴ This type of design experimentation, if used to deceive consumers or manipulate them into taking unwitting or detrimental actions, is a signal of dark patterns at work.¹⁵

...the use of manipulative design techniques in the digital world can pose heightened risks to consumers.

An example of this design experimentation is in the FTC’s action against Credit Karma.¹⁶ Credit Karma advertises third-party financial products, such as credit cards, and provides links for consumers to apply for offers. Credit Karma conducted A/B testing, which is an experiment where a company shows consumers two or more variants of something, such as an advertisement or a webpage, to determine which one performs better. Credit Karma compared how consumers reacted to being told that they had been “pre-approved” for a credit card (a false claim, according to the FTC’s complaint) versus being told that they had “Excellent” odds of being approved. The company ultimately decided to employ the allegedly false “pre-approved” claim, which the A/B testing had shown yielded a greater click rate.¹⁷

Dark patterns can be found in a variety of industries and contexts, including ecommerce, cookie consent banners, children’s apps, subscription sales, and more.

Dark patterns can be found in a variety of industries and contexts, including ecommerce, cookie consent banners, children’s apps, subscription sales, and more.¹⁸ (See Appendix A.) The specific types of dark patterns consumers are most likely to face differ depending on the types of websites or apps they frequently use.¹⁹ The medium through which consumers access online information also affects the number and types of dark patterns they may encounter. Studies show that some dark patterns are more common in mobile apps than on websites.²⁰ Additionally, some design techniques are more effective on smaller screens than on larger ones. Many companies, for instance, are able to hide important information from consumers on their mobile devices because the amount of scrolling required makes it unlikely that people will see it.²¹ Such dark patterns may have a differential impact on lower-income consumers or other vulnerable populations who are more likely to rely on a mobile device as their sole or primary access to the internet.²² Workshop panelists and researchers in the field note that dark patterns may also appear in new and evolving modalities such as augmented reality (AR) and virtual reality (VR) technologies, exposing consumers to manipulation on a whole new plane.²³

Dark patterns also raise special enforcement challenges. Because dark patterns are covert or otherwise deceptive, many consumers don’t realize they are being manipulated or misled.²⁴ Workshop participants theorized that even when consumers do realize they have been deceived, many don’t report their experiences, some out of an unnecessary feeling of embarrassment at being tricked.²⁵ That is why the FTC’s workshop brought together enforcement agencies, academic researchers, and consumer advocates to share their knowledge of dark patterns, explore whether they harm consumers, and, when practices were identified as unfair or deceptive, how to best address and eliminate them. In this paper, we shine a further light on some common dark patterns and the harms they cause consumers, while putting businesses on notice that the FTC will continue scrutinizing these practices.

Common Dark Patterns & Consumer Protection Concerns

In this section, we describe examples of common dark patterns—using recent FTC enforcement actions as well as insights from workshop participants—to illustrate the harms posed to consumers and provide recommendations for businesses.

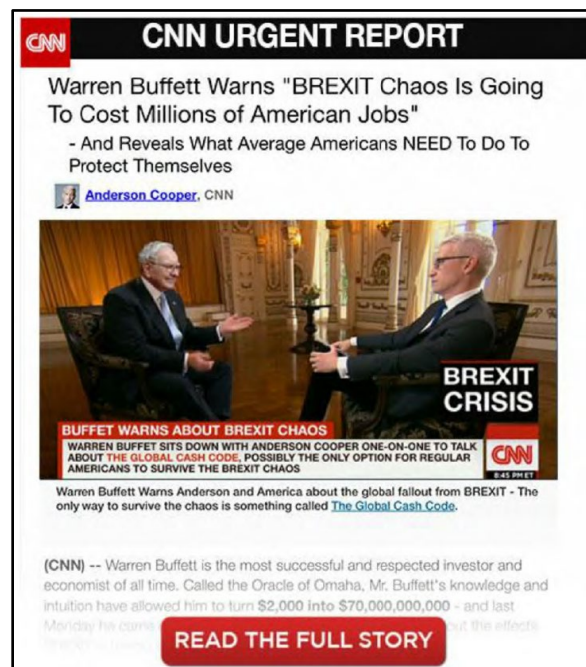
I. Design Elements that Induce False Beliefs

Some dark patterns manipulate consumer choice by inducing false beliefs.²⁶ For example, a company may make an outright false claim or employ design elements that create a misleading impression to spur a consumer into making a purchase they would not otherwise make. Classic examples of these types of deceptive dark patterns include advertisements deceptively formatted to look like independent, editorial content²⁷ and purportedly neutral comparison-shopping sites that actually rank companies based on compensation.²⁸ Workshop panelists also discussed countdown timers on offers that are not actually time-limited,²⁹ claims that an item is almost sold out when there is actually ample supply,³⁰ and false claims that other people are also currently looking at or have recently purchased the same product.³¹

...disguised advertising and promotional messages are deceptive when they mislead consumers into believing they are independent, impartial, or not from the sponsoring advertiser itself.

The FTC long has taken action against dark patterns involving companies that use ads deceptively formatted to look like news articles to entice consumers to buy their products.³² As explained in the FTC’s Enforcement Policy Statement on Deceptively Formatted Ads, disguised advertising and promotional messages are deceptive when they mislead consumers into believing they are independent, impartial, or not from the sponsoring advertiser itself.³³ A recent example is an FTC action charging Effen Ads, the operators of a work-from-home scheme, with using fake news stories to trick consumers into buying their program.³⁴ According to the complaint, Effen Ads sent unsolicited emails to consumers that included “from” lines that falsely claimed they were coming from news organizations like CNN or Fox News.³⁵

Figure 1: Effen Ads

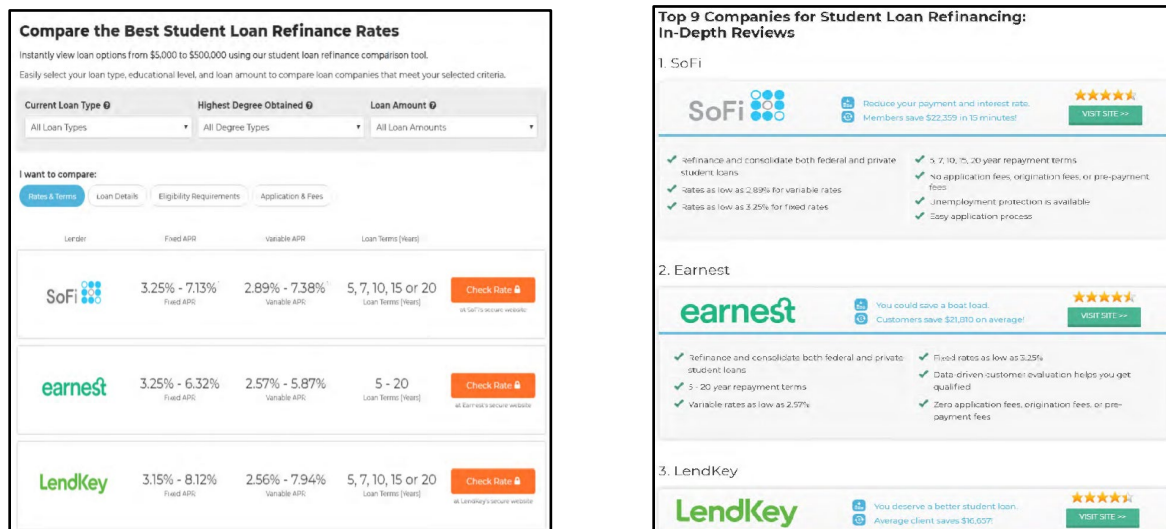


The FTC's complaint states that consumers who clicked on the links in these emails were routed to additional fake online news stories, and then eventually routed to Effen Ads' sales websites, which pitched the company's work-from-home schemes.³⁶ These sites guaranteed consumers would make hundreds of dollars if they paid an upfront fee of \$97 and worked from home only one hour a day. In reality, according to the complaint, the emailed articles were fake, and the upfront fee didn't result in an actual job.³⁷

Comparison websites can also induce false beliefs in consumers when the overall net impression created by various design elements is deceptive.³⁸ For example, consumers who visit websites where companies have created rankings lists, posted consumer reviews, or otherwise endorsed third parties expect these recommendations to be objective and unbiased.³⁹ When they aren't—and instead are based on whether the third parties are paying to be promoted, a personal relationship, or other connections—these sites are deceptive. These supposedly neutral rankings sites are using a dark pattern to manipulate consumer choice.⁴⁰ Knowing that there is a payment relationship or other connection between the reviewer and the third party would affect the weight or credibility consumers give the review and may influence whether and to what extent consumers choose to interact with that content at all.⁴¹ Deceptive ranking sites may also undermine fair competition, disadvantaging those companies that won't pay-to-play.⁴²

The FTC's action against the loan comparison website LendEDU.com is instructive.⁴³ As detailed in the FTC complaint, LendEDU used its rankings to sort companies in rate comparison tables, thereby giving consumers the impression that LendEDU had evaluated the top-listed company to be the best.⁴⁴

Figure 2: LendEDU Rate Comparison Tables



In reality, the FTC alleged, LendEDU boosted companies' numerical rankings and positions on rate tables based exclusively on how much they paid LendEDU.⁴⁵ Also, as alleged in the complaint, LendEDU falsely represented to consumers that its rankings of financial services companies were "objective," "honest," "accurate," and "unbiased."⁴⁶ Well aware of the effect on consumers, LendEDU employees enticed lenders to pay more by touting statistics showing that consumers were more likely to click on companies in better positions, according to the FTC's complaint.⁴⁷

To comply with the FTC Act, companies should make certain that their online interfaces do not create false beliefs or otherwise deceive consumers. Companies are on the hook for the net impression conveyed by the various design elements of their websites, not just the veracity of certain words in isolation.⁴⁸ For example, companies shouldn't give the impression that a ranking or review is objective and unbiased if it is based on or affected by third-party compensation.⁴⁹ And if an advertisement strongly resembles editorial content such as a news article, or appears formatted as native content in a publication with a strong journalistic brand, it is unlikely disclaimers will overcome the deceptive net impression.⁵⁰ Overall, when designing user interfaces, businesses should look not just at the effect their design choices have on sales, click-through rates, or other profit-based metrics, but also on how those choices affect consumers' understanding of the material terms of the transaction.⁵¹ And if a business becomes aware that a particular design choice manipulates consumer behavior by inducing false beliefs, the company should remediate the problem.

Overall, when designing user interfaces, businesses should look not just at the effect their design choices have on sales, click-through rates, or other profit-based metrics, but also on how those choices affect consumers' understanding of the material terms of the transaction.

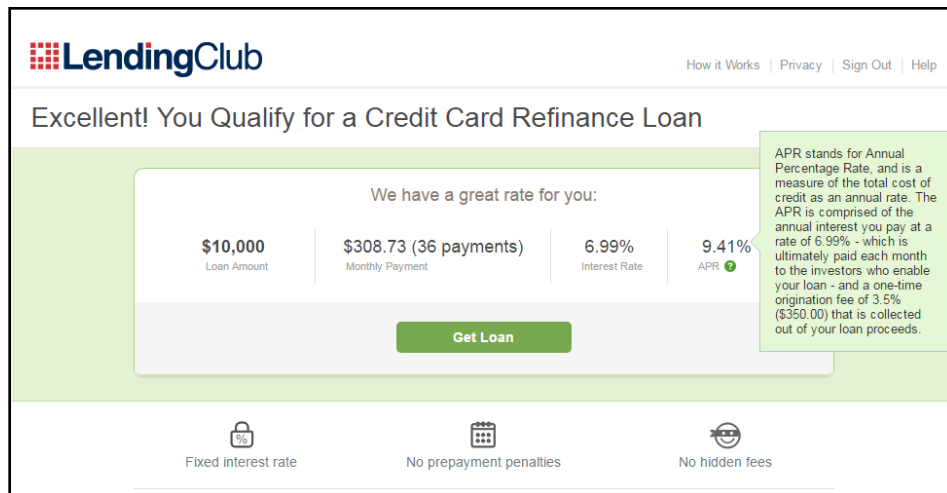
II. Design Elements that Hide or Delay Disclosure of Material Information

Some dark patterns operate by hiding or obscuring material information from consumers, such as burying key limitations of the product or service in dense Terms of Service documents that consumers don't see before purchase.⁵²

Similarly, some dark patterns trick people into paying hidden fees. For example, the FTC charged that the LendingClub Corporation deceived consumers about hidden fees associated with its online loans.⁵³ According to the FTC's complaint, LendingClub used prominent visuals to falsely promise loan applicants that they would receive a specific loan amount and pay "no hidden fees," when in reality the company deducted hundreds or even thousands of dollars in hidden fees from the loans it disbursed.⁵⁴

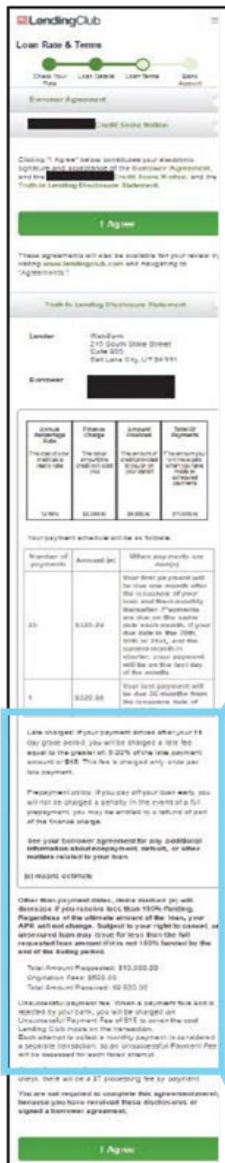
The FTC's complaint lays out how LendingClub hid the existence of its fees. LendingClub used tooltip buttons⁵⁵ consumers were unlikely to click on during the online application process, and buried mention of fees later in the application process in an un-bolded itemization sandwiched between more prominent, bolded paragraphs.⁵⁶ Furthermore, according to the FTC, in standard screen configurations, the fees appeared "below the fold" and thus required scrolling to be visible.⁵⁷ Consumers frequently reported that they only discovered the fee after LendingClub disbursed their loan proceeds, upon seeing that the disbursement amount was smaller than expected.⁵⁸

Figure 3: LendingClub Tooltip



On mobile devices, information about the upfront fee and total amount received was not displayed until the consumer had scrolled down approximately four times, depicted below.

Figure 4: LendingClub Mobile Application Process



Late charges: If your payment arrives after your 15 day grace period, you will be charged a late fee equal to the greater of: 5.00% of the late payment amount or \$15. This fee is charged only once per late payment.

Prepayment policy: If you pay off your loan early, you will not be charged a penalty. In the event of a full prepayment, you may be entitled to a refund of part of the finance charge.

See your borrower agreement for any additional information about nonpayment, default, or other matters related to your loan.

(e) means estimate

Other than payment dates, items marked (e) will decrease if you receive less than 100% funding. Regardless of the ultimate amount of the loan, your APR will not change. Subject to your right to cancel, an unsecured loan may issue for less than the full requested loan amount if it is not 100% funded by the end of the listing period.

Total Amount Requested: \$10,000.00
Origination Fees: \$500.00
Total Amount Received: \$9,500.00

Unsuccessful payment fee. When a payment fails and is rejected by your bank, you will be charged an Unsuccessful Payment Fee of \$15 to cover the cost Lending Club incurs on the transaction. Each attempt to collect a monthly payment is considered a separate transaction, so an Unsuccessful Payment Fee will be assessed for each failed attempt.

Another variation on the hidden-fee dark pattern is “drip pricing,” in which firms advertise only part of a product’s total price to lure in consumers, and do not mention other

mandatory charges until late in the buying process. Drip pricing interferes with consumers' ability to price-compare and manipulates them into paying fees that are either hidden entirely or not presented until late in the transaction, after the consumer already has spent significant time selecting and finalizing a product or service plan to purchase.⁵⁹ Panelists at the FTC's workshop discussed how consumers feel committed to a purchase by the time they reach the checkout screen, and feel "really frustrated that, when they begin this process, they have no idea how much it costs until it's too late."⁶⁰

Drip pricing costs consumers money—one study compared consumer expenditures on a ticketing website that uses drip pricing versus one that disclosed mandatory fees upfront and found that "users who weren't shown the ticket fees upfront ended up spending about 20% more money and were 14% more likely to complete [the transaction]."⁶¹ Drip pricing can also weaken competition by making it harder for consumers to price-compare across sellers.⁶² An honest business that sets forth the total price of its product at the outset will be at a significant disadvantage when compared to a seller that advertises an artificially low price to draw consumers in, then adds mandatory charges late in the transaction. As discussed at the workshop, companies should include any unavoidable and mandatory fees in the upfront, advertised price, and failure to do so has the potential to deceive consumers in violation of the FTC Act.⁶³ Relatedly, companies must not mislead consumers to believe that fees are mandatory when they are not.⁶⁴

...companies should include any unavoidable and mandatory fees in the upfront, advertised price, and failure to do so has the potential to deceive consumers in violation of the FTC Act.

Further, particularly where the drip pricing practices involve a credit product, companies must make sure their practices don't treat consumers differently on the basis of race, national origin, or another protected characteristic.⁶⁵ The FTC has brought several actions against brick-and-mortar retailers engaged in dark patterns involving drip pricing, charging companies with violations of the FTC Act and ECOA.⁶⁶ Additionally, companies whose sales practices target a specific audience, such as children, older adults, or native speakers of other languages, must take into consideration how their claims and design choices will be perceived by these groups.⁶⁷ For example, if a business markets a product to older adults, it should avoid design elements that are harder for older consumers to perceive, such as putting important information at the periphery of the screen or in a light color.⁶⁸ Also problematic are disclosures made with poor color contrast, such as a white-text disclosure on a yellow background.⁶⁹ Failing to factor this in can lead to law violations, including of the FTC Act and COPPA.⁷⁰

...particularly where the drip pricing practices involve a credit product, companies must make sure their practices don't treat consumers differently on the basis of race, national origin, or another protected characteristic.

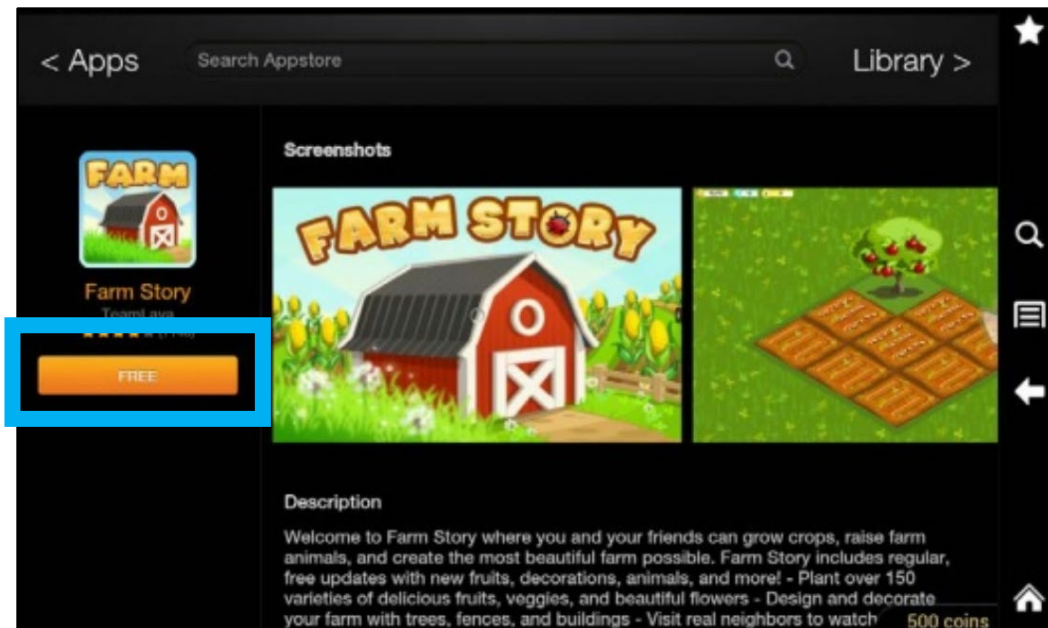
III. Design Elements that Lead to Unauthorized Charges

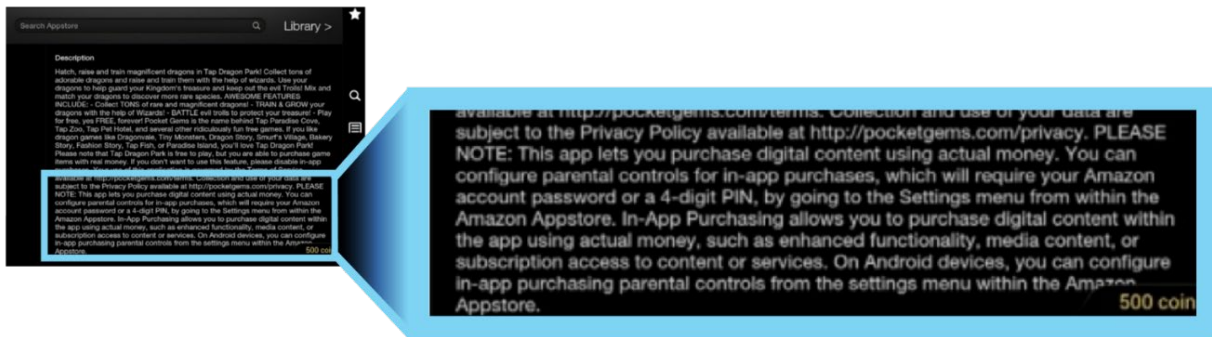
Another common dark pattern involves tricking someone into paying for goods or services that they did not want or intend to buy, whether the transaction involves single charges or recurring charges.⁷¹ Along with wasting consumers' time and money, these dark patterns can undermine consumer trust in the market, ultimately hurting other companies who engage in legitimate and honest practices.⁷²

Several workshop panelists raised concerns about dark patterns that result in unauthorized charges. One panelist explained how dark patterns can be deployed in children's gaming apps: "Let's say the green button is the button they click to advance from one level to the next level. And then suddenly, that button is suddenly a 'Buy' button. Most children will have been caught, because they've been clicking, clicking, clicking, clicking, and suddenly that's a 'Buy' button."⁷³

The FTC has brought enforcement actions against companies involving kids' in-app charges. This was the central issue in the FTC's actions against Amazon, Apple, and Google.⁷⁴ Amazon, for example, charged parents and other account holders for kids' purchases in mobile apps hosted on its app store.⁷⁵ The company advertised kids gaming apps as "free" while burying in fine-print on app description pages the fact that app users could make in-app purchases.⁷⁶

Figure 5: Amazon App Store Example





Once the account holder downloaded the app and children began playing the game, unbeknownst to the account holder, kids could simply rack up multiple charges, ranging from \$0.99 to \$99.99 each, by tapping buttons, with no account holder involvement. These purchases were often disguised as play. As explained by the judge in the case decision, “a child may be prompted to use or acquire seemingly fictitious currency, including a ‘boatload of doughnuts, a can of stars, and bars of gold,’ but in reality the child is making an in-app purchase using real money.”⁷⁷ Amazon later added a password prompt for account holders only for in-app purchases of \$20 or more, and eventually added one in other situations, though not consistently. However, even that prompt failed to disclose that authorizing a single purchase also authorized unlimited purchases for the next 60 minutes.⁷⁸ Ultimately, Amazon was forced to make more than \$70 million in refunds available to consumers.⁷⁹

Another frequent example of a dark pattern resulting in unauthorized charges is when a company deceptively offers a free trial period, but then, unbeknownst to the consumer, the trial is followed by a recurring subscription charge if the consumer fails to cancel. One workshop panelist discussed his research on dark patterns in the context of a free trial offer. A control group of consumers was told they would receive a one-month free trial of data protection followed by monthly charges if they failed to cancel, while the “hidden information” group was told they would receive a one-month free trial and that terms and conditions apply. For the latter group, the automatic monthly charge information was included only in small gray font at the bottom of the page.⁸⁰ The dark pattern was highly effective. More than twice as many consumers in the hidden information group accepted the free trial offer as compared to consumers in the control group.⁸¹

Seeing a rise in these types of dark patterns, the FTC hosted a workshop⁸² in 2007 to analyze the marketing of goods and services through offers with negative option⁸³ features, then issued a staff report in 2009 that set forth principles to guide sellers offering negative options online.⁸⁴ Following this guidance, and years of FTC cases tackling negative option-related deception under the FTC Act and the Negative Option Rule,⁸⁵ Congress enacted the Restore Online Shoppers’ Confidence Act (“ROSCA”) in 2010.⁸⁶ ROSCA prohibits charging for goods and services sold over the internet using a negative option feature unless the seller (1) clearly and conspicuously discloses all material terms of the transaction before obtaining the consumer’s billing information; (2) obtains a consumer’s express informed consent before charging the consumer’s account; and (3) provides simple mechanisms for a consumer to stop recurring charges.⁸⁷ Since then, the FTC has used ROSCA as an additional tool to challenge a variety of

harmful negative option practices that saddle consumers with recurring payments for products and services they never intended to purchase or that they do not wish to continue purchasing.⁸⁸

The FTC’s first action alleging ROSCA violations charged Health Formulas, LLC, and several related companies and individuals with advertising “free” trial offers for dietary supplements, but then automatically charging those who signed up \$60-\$210 per month after the free trial unless they took action to cancel.⁸⁹ According to the complaint, the free trial was prominently displayed, while the monthly charges were buried in the middle of smaller, dense font.⁹⁰

Figure 6: Health Formulas Example

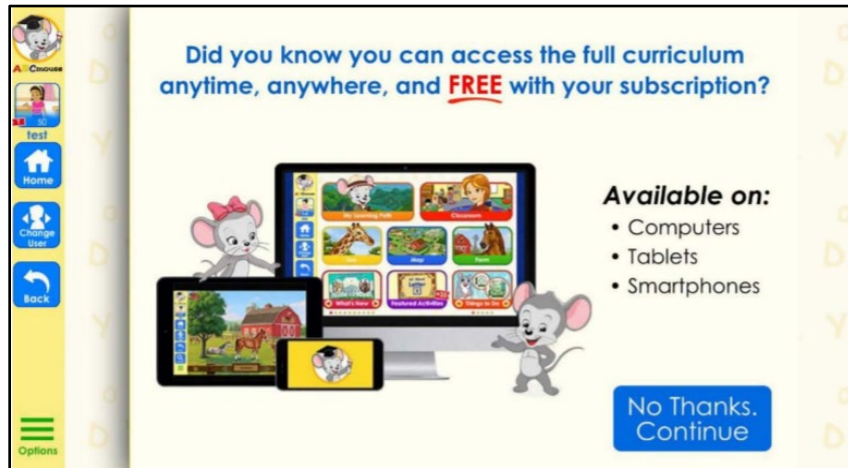


product. If you are satisfied with our product, then do nothing—we will bill you \$79.97 for your initial order, and every thirty days thereafter we will send you a new 30-day supply of our product, and automatically bill you the low price of \$79.97. To cancel

A related dark pattern makes it hard for consumers to cancel subscription services, resulting in ongoing recurring charges.⁹¹ The FTC’s complaint against ABCMouse, the operators of a children’s online learning site, offers a particularly striking example of how dark patterns can be used to block consumers’ cancellation attempts.⁹² According to the FTC, ABCMouse enrolled consumers into 30-day free trials or into 6- or 12-month memberships and, despite promising “Easy Cancellation,” many consumers could not cancel even after repeated attempts at calling, emailing, and contacting ABCMouse through a customer support form.⁹³

The complaint alleges that the company rejected any cancellation attempt through one of these methods and instead required consumers to navigate a difficult-to-find, lengthy, and confusing cancellation path on the website.⁹⁴ Consumers allegedly had to click through several pages of promotions and links that, when clicked, directed consumers away from the cancellation path without warning.⁹⁵ For example, the first screen in the path, depicted below, did not mention the word cancellation anywhere or tell consumers that they had arrived at the correct place to cancel:

Figure 7: First Screen in ABCmouse Cancellation Path



Another screen in the cancellation path offered consumers a “special Upgrade offer.” Only by clicking the “Continue” button could consumers proceed with cancellation, even though, according to the FTC’s complaint, the screen appeared to be an offer for a different product.

Figure 8: Another of Several Screens in ABCmouse Cancellation Path



In total, the FTC alleged that ABCMouse required consumers to navigate between six and nine screens to cancel their memberships, and consumers could not skip ahead or cancel without visiting each screen.⁹⁶ Further, according to the FTC, each screen included multiple links and buttons that, if pressed, would take consumers out of the cancellation path altogether.⁹⁷ This is a prime example of what one workshop panelist referred to as “sludge”: “a high friction experience that, by its nature, causes people to become fatigued and give up.”⁹⁸ It is also a dark pattern, an unfair practice under the FTC Act, and a ROSCA violation arising from the failure to provide a simple mechanism to cancel.⁹⁹

How can a company obtain express informed consent from consumers before charging them? The answer depends on the circumstances,¹⁰⁰ but at a minimum, companies looking to stay on the right side of the law should make sure their procedures for obtaining consent include an affirmative, unambiguous act by the consumer.¹⁰¹ Companies should not hide key terms of a purchase in a general terms and conditions document or behind hyperlinks, pop-ups, or drop-down menus.¹⁰² Acceptance of a general terms of use document that contains unrelated information does not constitute affirmative, unambiguous consent to a particular purchase. Likewise, manipulating consumers into agreeing by employing digital dark patterns designed to subvert their autonomy or impair their decision-making does not effectuate express informed consent.

Companies looking to stay on the right side of the law should make sure their procedures for obtaining consent include an affirmative, unambiguous act by the consumer.

Companies should ensure they obtain the express informed consent of the *accountholder* to any charges. This point is critical in mobile apps and games often played by children, where the accountholder may be a parent or someone other than the child who is playing the game. This is also an important consideration for consumers who may have multiple adults sharing a device.¹⁰³

Companies should ensure they obtain the express informed consent of the accountholder to any charges.

With respect to cancellation, as explained in the FTC’s Enforcement Policy Statement on Negative Option Marketing, ROSCA requires online negative option sellers to provide a simple mechanism for consumers to cancel.¹⁰⁴ To meet this standard, negative option sellers should provide cancellation mechanisms that are at least as easy to use as the method the consumer used to buy the product or sign up for the service.¹⁰⁵ This means that consumers should be able to cancel their subscription through the same medium (such as a website or mobile application) that the consumer used to sign up for the negative option plan in the first place.¹⁰⁶ It also means that negative option sellers should not subject consumers to new offers or similar attempts to save the

account that impose unreasonable delays on consumers' cancellation efforts.¹⁰⁷ In addition, if the seller provides for telephone cancellation, it should, at a minimum, answer all calls to its cancellation number during normal business hours, within a short time frame.¹⁰⁸ Calls to cancel should not be lengthier or otherwise more burdensome than the telephone call the consumer used to sign up.

...negative option sellers should provide cancellation mechanisms that are at least as easy to use as the method the consumer used to buy the product or sign up for the service.

IV. Design Elements that Obscure or Subvert Privacy Choices

Another pervasive dark pattern involves design elements that obscure or subvert consumers' privacy choices. Because of dark patterns, consumers may be unaware of the privacy choices they have online or what those choices might mean.¹⁰⁹ This may result in a significant deviation from consumers' actual privacy preferences.¹¹⁰

The FTC has been addressing dark patterns through privacy cases and policy work for many years. Workshop panelists noted that dark patterns that subvert consumer privacy preferences often take the form of a purported choice offered to consumers related to their data, except that choice is illusory and presented in a way that nudges consumers toward increased data sharing.¹¹¹ As discussed in further detail below, workshop panelists discussed how companies incorporate dark patterns into their products in various ways, including through user interfaces that:

- (1) do not allow consumers to definitively reject data collection or use;
- (2) repeatedly prompt consumers to select settings they wish to avoid;
- (3) present confusing toggle settings leading consumers to make unintended privacy choices;
- (4) purposely obscure consumers' privacy choices and make them difficult to access;
- (5) highlight a choice that results in more information collection, while greying out the option that enables consumers to limit such practices; and
- (6) include default settings that maximize data collection and sharing.

The workshop panelists discussed various examples of dark patterns relating to information collection. For instance, one panelist pointed to the commonly used cookie consent dialogue—presenting the consumer with the option whether to allow the company to set a cookie—as one example of a user interface that highlights the company's preferred choice while greying out the disfavored option.¹¹² This interface “places the option to accept cookies front and center, while the option to deny or modify cookie settings is usually behind, perhaps, several different screens.”¹¹³ Another researcher noted that even where users are asked to provide

consent, they are often not informed in a clear and understandable way about the practices that they are being asked to approve.¹¹⁴

The workshop panelists also discussed examples of interfaces that maximize information collection and sharing, such as using default settings to make consumer data collection difficult to avoid, even when such collection is unnecessary.¹¹⁵ One researcher explained that companies now frequently collect mobile phone numbers by default; she argues these numbers have become “the new Social Security number” because consumers so rarely change them.¹¹⁶ As such, she stated that mobile numbers are seldom actually needed for the provision of an online service, but “companies are often eager to get those [numbers] because it’s another way they can identify you,” and target you with advertising.¹¹⁷ Another example of a default setting maximizing data collection discussed at the workshop was the set-up flow for Google’s Android phones, which the researcher argued encourages consumers to enable location collection because “the way [Google] portrayed the choices was in such a manner that you would turn on location tracking.”¹¹⁸ As the researcher explained, location data is extremely valuable and can reveal sensitive details about consumers including where they live and work and even their sexual orientation or political and religious affiliations.¹¹⁹ In fact, the FTC sued data broker Kochava, Inc., related to its sale of consumer location data.¹²⁰ The FTC alleged in its complaint that Kochava sold geolocation data from hundreds of millions of mobile devices—data that can be used to trace the movements of individuals to and from sensitive locations, including reproductive health clinics, places of worship, and domestic violence shelters, among others.¹²¹ Thus, subverting a consumer’s privacy intentions with respect to location information would be highly problematic.

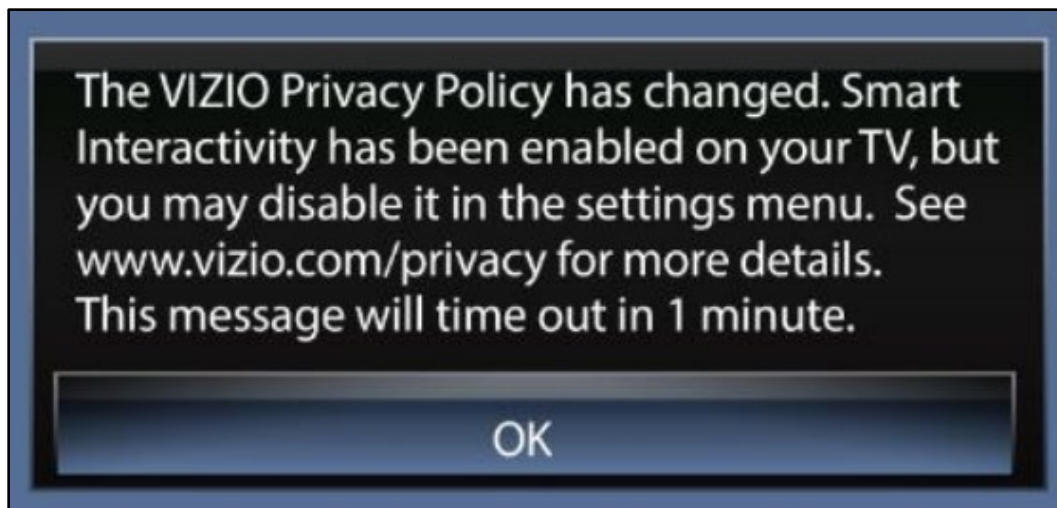
...subverting a consumer’s privacy intentions with respect to location information would be highly problematic.

In addition to the dark patterns discussed at the workshop, the recent FTC Staff Report on the privacy practices of major internet service providers (“ISPs”)¹²² pointed to similar dark patterns in those companies’ user interfaces.¹²³ First, certain ISPs included interfaces where the ISP’s preferred choice was highlighted while the alternative (less favorable to the ISP) was greyed out (e.g., the “Accept” choice is in a bold, blue background, while “Reject” is in muted grey, almost resembling an inactive button).¹²⁴ The Staff Report explained how such an interface may indicate to consumers that they have no choice but to select “Accept,” or might lead consumers to select “Accept” out of expediency without realizing their ability to “Reject” due to the difference in prominence of the two choices. Second, the Report highlighted interfaces that do not allow consumers to reject data collection or that continuously prompt consumers if they select a disfavored setting. For example, a consumer may be asked to either “accept” the collection of their location information or choose “remind me later,” which leads to repeated prompting until a consumer finally succumbs and accepts—likely out of frustration.¹²⁵

Notably, in this situation, the company does not even give a consumer an option to reject data collection altogether. Third, consumer privacy choices may be buried or hidden from consumers, forcing them to search through a number of tabs and sub-tabs in order to review and change their privacy preferences.¹²⁶ Finally, the report found unclear toggle settings that can confuse consumers into selecting a privacy setting they did not intend. For example, a “Do Not Sell My Information” option followed by an “off” toggle creates a double negative and might make it unclear whether consumers need to toggle the setting on or off to prohibit the sale of their information.¹²⁷

In addition to our workshops and our ISP 6b study, the FTC has brought cases against companies that use dark patterns to subvert consumer privacy choices. One example is the Commission’s case against Vizio, a smart-TV manufacturer. In *Vizio*,¹²⁸ the FTC alleged that the company enabled a default setting called “Smart Interactivity,” which enabled consumers to receive “program offers and suggestions,” but in reality allowed Vizio to comprehensively collect and share consumers’ television viewing activity with third parties. The complaint stated that Vizio provided no notice of this default setting to many of its consumers.¹²⁹ At a certain point, it provided the below notice to some consumers, which timed out after one minute and provided no direct link to the settings menu or privacy policy.¹³⁰ In any event, the FTC alleged that by keeping the setting name vague, Vizio effectively removed consumers’ ability to make an informed choice about their data sharing.¹³¹ The alleged conduct was a clear example of a dark pattern that subverted consumers’ privacy choices.

Figure 9: Vizio Privacy Notice



Businesses should, first and foremost, aspire to become good stewards of consumer personal information. Data minimization measures should be inherent in any business plan—this makes sense not only from a consumer privacy perspective, but also from a business perspective

because it reduces the risk of liability due to potential data exposure. Businesses should collect the data necessary to provide the service the consumer requested, and nothing more.

Businesses should, first and foremost, aspire to become good stewards of consumer personal information.

In addition to generally minimizing data collection efforts, businesses should also avoid subverting consumers' privacy choices. First, companies should avoid default settings that lead to the collection, use, or disclosure of consumers' information in a way that they did not expect (and collect information only when the business has a justified need for collecting the data). Second, companies should make consumer choices easy to access and understand. Consumers should not have to navigate through multiple screens to find privacy settings or have to look for settings buried in a privacy policy or in a company's terms of service: they should be presented at a time and in a context in which the consumer is making a decision about their data. Any toggle options presented to the consumer should not be ambiguous or confusing, and one option should not be more prominent than another. Third, choices about sensitive information, in particular, should be presented so that it is clear to the consumer what they are consenting to – as opposed to a blanket consent – and should be presented along with information that they need to make an informed decision (for example, that if the consumer consents to the collection of their information, that information will be shared with third parties). More generally, businesses should take a moment to 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.

Consumers should not...have to look for settings buried in a privacy policy or in a company's terms of service: they should be presented at a time and in a context in which the consumer is making a decision about their data.

Another variation on the privacy-related dark pattern involves lead generators that convey a false affiliation to manipulate consumers into sharing personal information. For example, the FTC charged the lead generator Sunkey Publishing¹³² with using websites such as army.com and armyenlist.com, designed to appear as official recruiting websites affiliated with the U.S. military, to target people seeking to join the armed forces and trick them into submitting their information. According to the FTC complaint, Sunkey falsely promised to use the information collected only for military recruitment purposes and not to share it with anyone else.¹³³

Figure 10: Sunkey Information Request Page

In reality, according to the complaint, Sunkey sold the information as marketing leads to post-secondary schools for \$15 to \$40 per lead, and consumers received follow-up phone calls from telemarketers giving consumers the false impression that the U.S. military actually endorsed those schools.¹³⁴ Similar examples of deceptive lead generator dark patterns can be found in the FTC’s cases against *EduTrek*,¹³⁵ *Blue Global*,¹³⁶ and *ITMedia*.¹³⁷

Lead generators must be honest about who they are and why they are collecting consumer information.

Lead generators must be honest about who they are and why they are collecting consumer information. If a company represents that they are collecting consumer information for one audience or one purpose, they cannot then share it with a different buyer or for a different purpose without consumer consent. Deceptive lead generators that manipulate consumers into sharing personal information under false pretenses violate the FTC Act. When the “product” a business sells includes sensitive data, they must take steps to vet prospective buyers and understand how that information is being used. Further, companies who use others to generate leads should monitor what those third parties are doing on their behalf and ensure the leads they use weren’t the product of deception.

Conclusion

While dark patterns may manipulate consumers in stealth, these practices are squarely on the FTC’s radar.

The FTC’s “Bringing Dark Patterns to Light” workshop and cases involving dark patterns represent the agency’s longstanding efforts to study and combat dark patterns and to raise awareness about the dangers they pose to consumers. This Staff Report serves as an additional resource for the public and a guide for businesses as they develop, design, and improve their online interfaces.

Firms that nonetheless employ dark patterns, take notice: where these practices violate the FTC Act, ROSCA, the TSR, TILA, CAN-SPAM, COPPA, ECOA, or other statutes and regulations enforced by the FTC, we will continue to take action.

Appendix A

Compilation of Digital Dark Patterns

Digital Dark Patterns are design practices that trick or manipulate users into making choices that they might not otherwise have made. Below are some common dark patterns identified by FTC workshop panelists and found in the academic literature.

Dark Pattern Type	Dark Pattern Variant	Description
ENDORSEMENTS (aka “SOCIAL PROOF”)	False Activity Messages	Making false claims about others’ activity on a site or interest in a product <i>Example: “24 other people are viewing this listing”</i>
	Deceptive Consumer Testimonials	Using phony customer endorsements or presenting other people’s experience without revealing material information, such as: (1) the endorsers were compensated; (2) the endorsers have a connection to the company, like being an employee or a family member; or (3) the endorsers’ experiences aren’t typical of what others will experience in similar circumstances
	Deceptive Celebrity Endorsements	Featuring testimonials that falsely appear to come from celebrities OR Using celebrities or prominent influencers to endorse a product without disclosing that the celebrity was paid for the endorsement or was given the product for free
	Parasocial Relationship Pressure	Using characters that children know and trust to pressure them into making a certain choice <i>Example: Using a well-known cartoon character to encourage children to make in-app purchases</i>
SCARCITY	False Low Stock Message	Creating pressure to buy immediately by saying inventory is low when it isn’t <i>Example: “Only 1 left in stock – order soon”</i>
	False High Demand	Creating pressure to buy immediately by saying demand

	Message	is high when it isn't <i>Example: "20 other shoppers have this item in their cart"</i>
URGENCY	Baseless Countdown Timer	Creating pressure to buy immediately by showing a fake countdown clock that just goes away or resets when it times out <i>Example: "Offer ends in 00:59:48"</i>
	False Limited Time Message	Creating pressure to buy immediately by saying the offer is good only for a limited time or that the deal ends soon – but without a deadline or with a meaningless deadline that just resets when reached
	False Discount Claims	Creating pressure to buy immediately by offering a fake "discounted" or "sale" price
OBSTRUCTION	Price Comparison Prevention	Keeping shoppers from easily comparing prices by bundling things, using different measures (price per unit v. price per ounce), or listing the price per payment (such as \$10 per week) without disclosing the total number of payments or overall cost
	Roadblocks to Cancellation	Making it easy to sign up but hard to cancel, by requiring people to go through tedious, time-consuming cancellation procedures <i>Example: letting people sign up online, but making them use another means to cancel</i> <i>Example: requiring that people cancel by phone but then concealing the phone number, short-staffing the cancellation line, opening the line during limited hours, or requiring people to listen to a sales pitch or upsell while trying to cancel</i>
	Immortal Accounts	Making it hard or impossible to delete an account
SNEAKING OR INFORMATION HIDING	Sneak-into-Basket	Automatically adding items to the shopping cart without a shopper's permission OR Tricking a shopper into buying unwanted items by using a pre-checked box
	Hidden Information	Hiding material information or significant product limitations from people <i>Example: hiding info in fine print, in lengthy terms of service documents, behind nondescript</i>

		<i>hyperlinks, or in pop-up boxes that only appear if someone hovers over the right thing</i>
	Hidden Costs	Adding hidden fees or other charges that people don't know about <i>Example: an undisclosed origination fee deducted from loan proceeds</i>
	Drip Pricing	Advertising only part of a product's total price initially and then imposing other mandatory charges late in the buying process <i>Example: a "convenience fee" that appears only when a shopper reaches the check-out screen</i>
	Hidden Subscription or Forced Continuity	Offering a free trial and, at the end of the trial, automatically and unexpectedly charging a recurring fee if consumers don't affirmatively cancel OR Offering a product for a small one-time fee, then automatically enrolling people into a subscription or continuity plan without their consent
	Intermediate Currency	Hiding the real cost by requiring consumers to buy things with virtual currency <i>Example: "coins" or "acorns" in kids' apps</i>
INTERFACE INTERFERENCE	Misdirection	Using style and design to focus users' attention on one thing in order to distract their attention from another <i>Example: presenting the subtotal price in a bright green highlighted box, then listing additional mandatory taxes and fees below in a non-highlighted section so users don't notice their final total will be higher</i>
	False Hierarchy or Pressured Upselling	In giving options, using contrasting visual prominence to steer users into making a certain selection <i>Example: during cancellation, presenting the "Keep My Subscription" option as a bright orange button, while presenting the "Cancel My Subscription" option as a smaller font, pale gray hyperlink hidden below the orange button</i>
	Disguised Ads	Formatting advertisements to falsely appear to be unbiased product reviews or independent journalism OR Presenting a ranking list, search engine, or comparison-

		shopping site as neutral and unbiased when it is actually based on advertising dollars
	Bait and Switch	A choice or interaction leads to an unexpected, undesirable outcome <i>Example: a user clicks the X in the top right corner of a pop-up but, instead of closing the box, it downloads software</i> <i>Example: selling a consumer something that turns out to be materially different than what was originally advertised</i>
COERCED ACTION	Unauthorized Transactions	Tricking people into paying for goods or services that they did not want or intend to buy, such as mislabeling the steps in a transaction or failing to obtain the express informed consent of the accountholder <i>Example: a shopping website button labeled "Next" that people think will lead to the next screen but, instead, processes the transaction immediately</i> <i>Example: a one-click button in children's gaming apps that charges parents real money</i>
	Auto-Play	Automatically playing another video once one video ends in a manner that is unexpected or harmful <i>Example: after the first video, a less kid-friendly video – or a sponsored ad camouflaged to look like a recommended video – automatically plays</i>
	Nagging	Asking repeatedly and disruptively if a user wants to take an action OR Making a request that doesn't let the user permanently decline – and then repeatedly prompting them with the request <i>Example: asking users to provide their data or turn on cookies then repeatedly presenting the choices as "Yes" or "Not Now" instead of "Yes" or "No"</i>
	Forced Registration or Enrollment	Making users create an account or share their information to complete a task <i>Example: "Create an account to continue with your purchase"</i>
	Pay-to-Play or	Saying that things are available with a purchase or

	<p>Grinding</p>	<p>download, but then charging users to actually obtain those things OR Making the free version of a game so cumbersome and labor-intensive that the player is induced to unlock new features with in-app purchases</p>
	<p>Friend Spam, Social Pyramid Schemes, and Address Book Leeching</p>	<p>Asking for an email address or social media permissions for one purpose but then using it for another OR Making users share information about people in their social network</p>
<p>ASYMMETRIC CHOICE</p>	<p>Trick Questions</p>	<p>Using ambiguity or confusing language – often double negatives – to steer a user to things they don’t want <i>Example: “Uncheck the box if you prefer not to receive email updates”</i> <i>Example: A checkbox next to the phrase “Decline the option of renewing your loan,” which if left un-checked is interpreted as acceptance of auto-renewal terms</i> <i>Example: when trying to cancel a subscription service, a button labeled “No, cancel” that doesn’t cancel your subscription but instead takes you out of the cancellation path</i></p>
	<p>Confirm Shaming</p>	<p>Using shame to steer users away from certain choices by framing the alternatives as a bad decision <i>Example: “No, I don’t want to save money” appears when a shopper selects a one-time purchase over a recurring one</i></p>
	<p>Preselection</p>	<p>Preselecting a default that’s good for the company, but not the user <i>Example: add-on products such as trip insurance or an extended warranty are automatically tacked on to a purchase unless the customer notices and opts out</i> <i>Example: the accept tracking cookies box is pre-checked</i> <i>Example: the site automatically shows shoppers the most expensive option, not the cheaper or free option</i></p>
	<p>Subverting Privacy</p>	<p>Tricking users into sharing more information than they</p>

	Preferences	really intended to <i>Example: asking users to give consent but not informing them in a clear, understandable way what they are agreeing to share</i> <i>Example: telling users the site is collecting their information for one purpose but then sharing it with others or using it for other purposes</i> <i>Example: including default settings that maximize data collection and making it difficult for users to find and change them</i> <i>Example: giving users a choice, but one where the "Accept" choice is in a bold, blue background, while "Reject" is greyed out and in small print</i>
--	--------------------	--

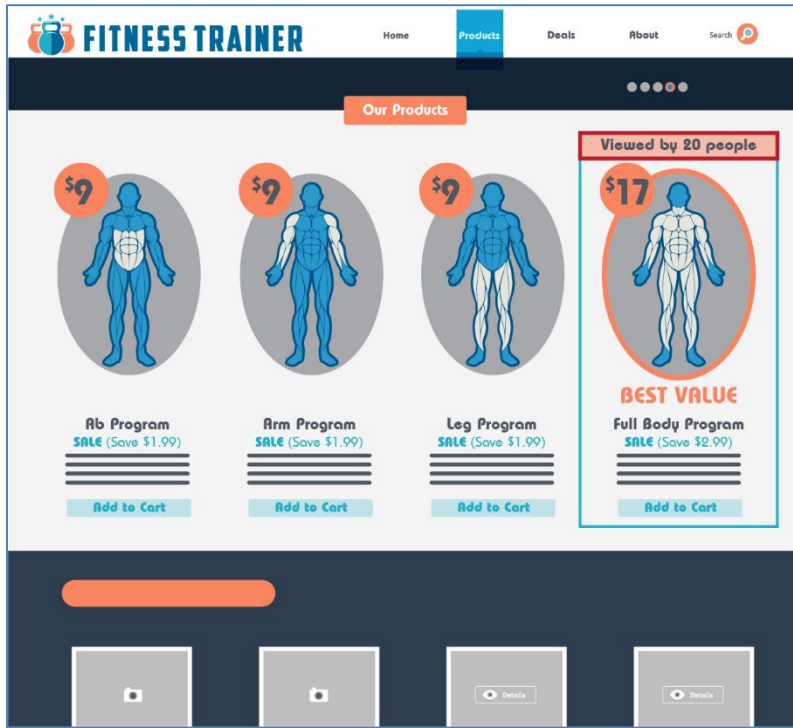
Appendix B

Even a single purchase can bring you into contact with many dark patterns. Here are some common ways that you can be tricked or manipulated during online transactions.



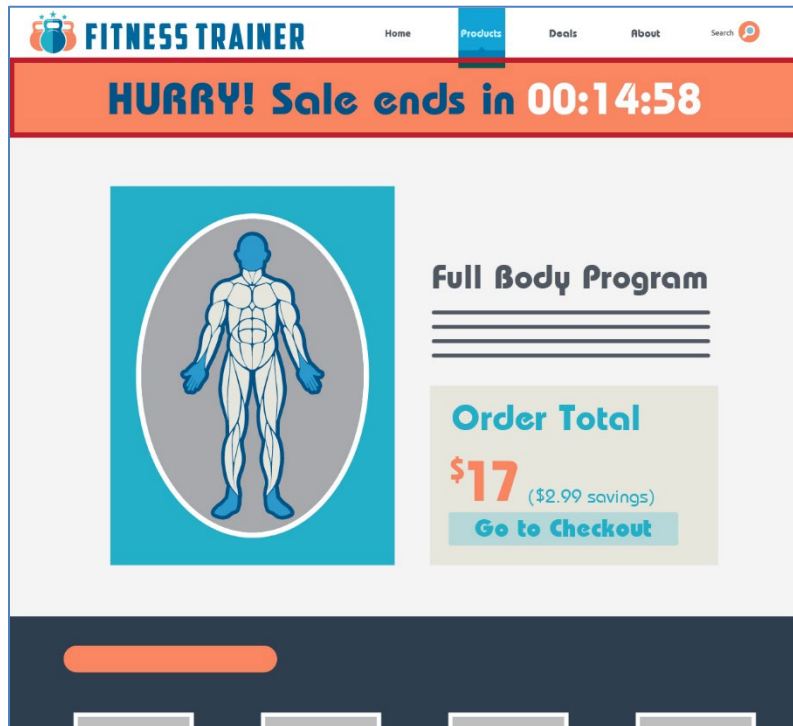
Sites can use design, style, and confusing language to steer you to a certain choice. This one wants you to share information – maybe more than you wanted.

*Trick Question,
Subverting Privacy Preferences*



This page lies about what others on the site are doing (“20 other people viewed this item”) in an effort to boost sales.

False Activity Messages



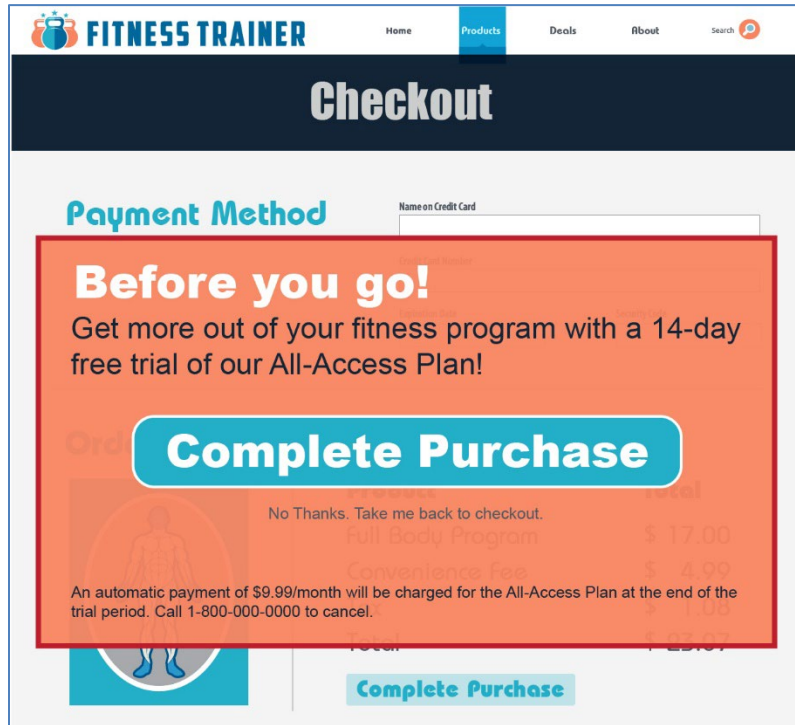
The fake countdown clock on this page pressures you to buy immediately, but the clock just goes away or resets when it times out.

Baseless Countdown Timer

Product	Total
Full Body Program	\$ 17.00
Convenience fee	\$ 4.99
Tax	\$ 1.08
Total	\$ 23.07

Here, an unexpected convenience fee of \$4.99 appears only right before you check out.

Drip Pricing



This promotion steers you to an unexpected subscription, charges a recurring fee even though the offer is advertised as a free trial, and only lets you cancel by phone.

*Pressured Upselling,
Hidden Information,
Hidden Subscription,
Roadblocks to Cancellation*

FITNESS TRAINER Home Products Deals About Search

Confirmation

Thank You for your order!

Order Number:	Order Date:	Payment Type:
00000000	01/01/2022	XXXX XXXX XXXX XXXX

Order Summary

Full Body Program	\$ 17.00
All-Access Program 14-Day Free Trial*	\$ 0.00
Convenience Fee	\$ 4.99
Tax	\$ 1.08
Total	\$ 23.07

*All-Access Program \$9.99/month subscription begins 01/15/2022.

This order confirmation page shows a recurring subscription fee in fine print at the bottom of the page that was snuck into your order on the prior page.

*Unauthorized Transaction,
Hidden Information*

Contributors

Division of Financial Practices

Stephanie Liebner
Brittany Frassetto
Eleni Broadwell
Samuel Jacobson
Sandhya Brown
Malini Mithal

Division of Privacy and Identity Protection

Gorana Neskovic
Mark Eichorn

Division of Consumer and Business Education

Marlena Patterson
Lesley Fair
Alvaro Puig

Division of Enforcement

Brad Winter

Division of Advertising Practices

Laura Sullivan
Annette Soberats

Endnotes

¹ See, e.g., European Commission, Directorate-General for Justice and Consumers, Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F., et al., *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation: final report* (May 2022), at 19, available at <https://data.europa.eu/doi/10.2838/859030> [hereinafter EU Dark Patterns Report] (“Persuasive practices and personalisation predate the online world and are also applied in the brick-and-mortar world. The digital transformation and the data economy, however, have made possible the adoption of these practices to an unprecedented level.”).

² In pursuance of this mission, the FTC administers a wide variety of laws and regulations, including the Federal Trade Commission Act. Section 5(a) of the FTC Act provides that “unfair or deceptive acts or practices in or affecting commerce . . . are . . . declared unlawful.” 15 U.S.C. Sec. 45(a)(1). “Deceptive” practices are defined in the FTC’s Deception Policy Statement as involving a material representation, omission, or practice that is likely to mislead a consumer acting reasonably under the circumstances. An act or practice is “unfair” if it “causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.” 15 U.S.C. Sec. 45(n).

³ See, e.g., *FTC v. Age of Learning, Inc., also d/b/a ABCmouse and ABCmouse.com*, Case No. 2:20-cv-07996 (C.D. Cal.); FTC Press Release, *Children’s Online Learning Program ABCmouse to Pay \$10 Million to Settle FTC Charges of Illegal Marketing and Billing Practices* (Sept. 2, 2020), at <https://www.ftc.gov/news-events/press-releases/2020/09/childrens-online-learning-program-abcmouse-pay-10-million-settle>; *FTC v. Prog Leasing, LLC, also d/b/a Progressive Leasing*, Case No. 1:20-cv-01668 (N.D. Ga.); FTC Press Release, *Rent-to-Own Payment Plan Company Progressive Leasing Will Pay \$175 Million to Settle FTC Charges It Deceived Consumers About Pricing* (April 20, 2020), at <https://www.ftc.gov/news-events/press-releases/2020/04/rent-to-own-payment-plan-company-progressive-leasing-will-pay-175>; *FTC v. LendingClub Corporation*, Case No. 3:18-cv-02454 (N.D. Cal.); FTC Press Release, *LendingClub Agrees to Pay \$18 Million to Settle FTC Charges* (July 14, 2021), at <https://www.ftc.gov/news-events/press-releases/2021/07/lendingclub-agrees-pay-18-million-settle-ftc-charges>; *FTC v. AH Media Grp.*, Case No. 3:19-cv-04022-JD (N.D. Cal.); FTC Press Release, *FTC Halts Online Subscription Scheme that Deceived People with “Free Trial” Offers* (May 8, 2020), at <https://www.ftc.gov/news-events/press-releases/2020/05/ftc-halts-online-subscription-scheme-deceived-people-free-trial>.

⁴ FTC, Enforcement Policy Statement Regarding Negative Option Marketing, 86 Fed. Reg 60822 (Oct. 28, 2021), available at https://www.ftc.gov/system/files/documents/public_statements/1598063/negative_option_policy_statement-10-22-2021-tobureau.pdf; FTC Press Release, *FTC to Ramp up Enforcement against Illegal Dark Patterns that Trick or Trap Consumers into Subscriptions* (Oct. 28, 2021), at <https://www.ftc.gov/news-events/press-releases/2021/10/ftc-ramp-enforcement-against-illegal-dark-patterns-trick-or-trap>.

⁵ FTC, “Bringing Dark Patterns to Light: An FTC Workshop,” <https://www.ftc.gov/news-events/events-calendar/bringing-dark-patterns-light-ftc-workshop>.

⁶ There are certain dark patterns that the FTC has consistently found to be unlawful, while others would depend on a case-by-case evaluation of all the attendant facts.

⁷ FTC, “Bringing Dark Patterns to Light: An FTC Workshop” Transcript, at 6, 8, https://www.ftc.gov/system/files/documents/public_events/1586943/ftc_darkpatterns_workshop_transcript.pdf [hereinafter “Dark Patterns Workshop Transcript”].

⁸ *Id.* at 28; Jamie Luguri, Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns* (March 23, 2021), *Journal of Legal Analysis*, Volume 13, Issue 1.

⁹ *See, e.g.*, EU Dark Patterns Report, at 39-40 (“A key issue that emerged from the research is that unfair commercial practices are rarely presented in isolation...The combination of several dark patterns is even more effective at influencing consumers’ choices, and complicates enforcement, which is often based on a practice-by-practice investigation.”); United Kingdom Competition & Markets Authority Discussion Paper, *Online Choice Architecture: How digital design can harm competition and consumers* (April 2022), at vi, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1066524/Online_choice_architecture_discussion_paper.pdf [hereinafter “CMA Online Choice Architecture Paper”] (“OCA practices are often not used in isolation, and tend to have stronger effects when they are combined.”).

¹⁰ FTC Complaint, *FTC v. RagingBull.com, LLC*, Case No 1:20-cv-3538 (D. Md.), available at https://www.ftc.gov/system/files/documents/cases/ragingbull.com_-_amended_complaint_for_permanent_injunction_and_other_equitable_relief.pdf.

¹¹ *See* Dark Patterns Workshop Transcript, at 34 (“When you move from a brick-and-mortar environment to a digital environment, there’s more aspects of the environment you can manipulate...you can also collect and leverage information about consumers.”). *See also* EU Dark Patterns Report, at 120 (“Dark patterns and manipulative personalisation practices can lead to financial harm, loss of autonomy and privacy, cognitive burdens, mental harm, as well as pose concerns for collective welfare due to detrimental effects on competition, price transparency and trust in the market.”).

¹² *See, e.g.*, Dark Patterns Workshop Transcript, at 33-37; EU Dark Patterns Report, at 20 (“The large-scale collection and analysis of personal data may be a threat not only for privacy but also due to the manner in which it is used to shape individual decision-making.”); CMA Online Choice Architecture Paper, at iii (“The speed and scale of data collection, experimentation, and targeted personalisation available to businesses online also facilitates the development and optimisation of choice architecture in real time.”); International Digital Accountability Council (“IDAC”), Public Comment Submitted to FTC on Dark Patterns Issues, FTC-2021-0019-0109, at 2, available at <https://www.regulations.gov/comment/FTC-2021-0019-0109>.

¹³ *See* Dark Patterns Workshop Transcript, at 37; Willis, L. E., *Deception by Design* (2020), *Harvard Journal of Law & Technology*, 34(1), 115-190 (“Although marketers have long used testing to predict which advertisements will be most effective, the difference between offline human-directed and online real-time machine-controlled experimentation is profound. The speed, scale, and thoroughness of machine experimentation ‘make[s] accessible a vast design space that ordinary human iteration wouldn’t be able to explore.”); EU Dark Patterns Report, at 20 (“Online platforms and traders gather data and then test different nudges. They see the reaction and steadily feed the information into machine learning algorithms that produce improved and refined nudges in a self-propelling cycle that is beneficial to them but may be detrimental for consumers.”).

¹⁴ *See* Dark Patterns Report Transcript, at 31, 34, 37.

¹⁵ Campaign for a Commercial-Free Childhood and The Center for Digital Democracy, Public Comment Submitted to FTC on Dark Patterns Issues, FTC-2021-0019-0108, at 1, 18-19, 30, available at <https://www.regulations.gov/comment/FTC-2021-0019-0108> [hereinafter Digital Democracy Public Comment].

¹⁶ *In the Matter of Credit Karma*, FTC Matter No. 2023138; FTC Press Release, *FTC Takes Action to Stop Credit Karma From Tricking Consumers With Allegedly False “Pre-Approved” Credit Offers* (Sept. 1, 2022), at <https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-takes-action-stop-credit-karma-tricking-consumers-allegedly-false-pre-approved-credit-offers>.

¹⁷ FTC Complaint, *In the Matter of Credit Karma*, FTC Matter No. 2023138, available at https://www.ftc.gov/system/files/ftc_gov/pdf/CK%20Complaint%209-1-22%20%28Redacted%29.pdf.

¹⁸ See Dark Patterns Workshop Transcript, at 2, 4, 6, 8, 18, 21, 57-59. See also EU Dark Patterns Report, at 45 (“Overall, mystery shoppers detected practices that they perceive as dark patterns in 73 out of the 75 websites and apps explored. Given that 97% of the websites/apps covered presented these practices, it is evident that the use of dark patterns is common across the board.”).

¹⁹ EU Dark Patterns Report, at 46-57.

²⁰ See Dark Patterns Workshop Transcript, at 10 (“We ultimately found the dark pattern count is frequently higher in apps than in websites, both when you look within a service or across types of the dark pattern.”); Gunawan, J., Pradeep, A., Choffnes, D., Hartzog, W., & Wilson, C., *A Comparative Study of Dark Patterns Across Mobile and Web Modalities* (2021). But see EU Dark Patterns Report, at 46 (“The prevalence of some dark patterns may thus differ depending on the modality...However, the mystery shopping exercise across 75 websites/apps found that the prevalence of dark patterns was generally similar in mobile apps and websites.”).

²¹ See Dark Patterns Workshop Transcript, at 75.

²² See generally Sara Atske & Andrew Perrin, *Home broadband adoption, computer ownership vary by race, ethnicity in the U.S.*, Pew Research Center (July 16, 2021), available at <https://www.pewresearch.org/fact-tank/2021/07/16/home-broadband-adoption-computer-ownership-vary-by-race-ethnicity-in-the-u-s/> (“A quarter of Hispanics are ‘smartphone-only’ internet users – meaning they own a smartphone but lack traditional home broadband services. By comparison, 12% of White adults fall into this category. Among Black adults, 17% are smartphone dependent, but this share is not statistically different from their White or Hispanic counterparts.”). See also Dark Patterns Workshop Transcript, at 9-11; Gunawan, J., Pradeep, A., Choffnes, D., Hartzog, W., & Wilson, C., *A Comparative Study of Dark Patterns Across Mobile and Web Modalities* (2021), at 23 (“Additionally, we are concerned that dark pattern variability across modalities may exacerbate existing social inequalities and exploit vulnerable populations, especially for people whose primary (or only) internet-capable device is mobile.”); IDAC Public Comment, *supra* note 12, at 1.

²³ See, e.g., Dark Patterns Workshop Transcript, at 19; EU Dark Patterns Report, at 60 (“Moreover, developments in the area of virtual or blended/augmented reality environments, such as the metaverse, generate additional potential for more immersive dark patterns and manipulative personalisation, which may differ significantly from the classic dark patterns or personalisation techniques used to date, and may have profound implications for consumer decision-making in the digital environment.”).

²⁴ See, e.g., Dark Patterns Workshop Transcript, at 73; EU Dark Patterns Report, at 85 (“Dark patterns are hidden, subtle and manipulative in nature, so it is difficult to spot and report them.”); CMA Online Choice Architecture Paper, at 42 (“When encountering a harmful OCA practice, such as a dark pattern, most individuals are unlikely to realise they were under the influence of a bias or heuristic that drove their decision making.”); Consumer Reports, Public Comment Submitted to FTC on Dark Patterns Issues, FTC-2021-0019-0119, at 3, available at <https://www.regulations.gov/comment/FTC-2021-0019-0119> (“By their very nature, dark patterns are difficult for consumers to identify.”).

²⁵ See, e.g., Dark Patterns Workshop Transcript, at 36; EU Dark Patterns Report, at 85 (“Another possibility is that a consumer who has been manipulated is embarrassed about being tricked and does not want to draw more attention to the problem.”).

²⁶ See Dark Patterns Workshop Transcript, at 8.

²⁷ See *id.* at 67-68, 75; See also FTC Enforcement Policy Statement on Deceptively Formatted Advertisements (Dec. 22, 2015), available at https://www.ftc.gov/system/files/documents/public_statements/896923/151222_deceptiveenforcement.pdf; *In the Matter of Lord & Taylor, LLC*, Docket No. C-4576; FTC Press Release, *Lord & Taylor Settles FTC Charges It Deceived Consumers Through Paid Article in an Online Fashion Magazine and Paid Instagram Posts by 50 “Fashion Influencers”* (March 15, 2016), at <https://www.ftc.gov/news-events/news/press-releases/2016/03/lord-taylor-settles-ftc-charges-it-deceived-consumers-through-paid-article-online-fashion-magazine>.

²⁸ See, e.g., *In the Matter of LendEDU, et al.*, Docket No. C-4719; FTC Press Release, *Operators of Comparison Shopping Website Agree to Settle FTC Charges Alleging Deceptive Rankings of Financial Products and Fake Reviews* (Feb. 3, 2020), at <https://www.ftc.gov/news-events/press-releases/2020/02/operators-comparison-shopping-website-agree-settle-ftc-charges>; *FTC v. Victory Media, Inc.*, Docket No. C-4640; FTC Press Release, *Victory Media Settles FTC Charges Concerning Its Promotion of Post-Secondary Schools to Military Consumers* (Oct. 19, 2017), at <https://www.ftc.gov/news-events/press-releases/2017/10/victory-media-settles-ftc-charges-concerning-its-promotion-post>. See also FTC Press Release, *FTC Puts Hundreds of Businesses on Notice about Fake Reviews and Other Misleading Endorsements* (Oct. 13, 2021), at <https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-puts-hundreds-businesses-notice-about-fake-reviews-other-misleading-endorsements>;

²⁹ Dark Patterns Workshop Transcript, at 8, 27. See also CMA Online Choice Architecture Paper, at 26 (“There is considerable evidence that consumers react to scarcity and divert their attention to information where they might miss opportunities... false or misleading scarcity claims, such as countdown clocks that reset or stock claims that are exaggerated or unsubstantiated, can put undue pressure on consumers to act.”)

³⁰ Dark Patterns Workshop Transcript, at 6, 72. See also CMA Online Choice Architecture Paper, at 26 (“Numerous experiments and studies find an effect of scarcity claims on click-through rates, purchase, perceived value, and favourability towards businesses who offer them.”) (citing to several academic research studies).

³¹ Dark Patterns Workshop Transcript, at 6, 27.

³² See e.g., *FTC v. Victory Media, Inc.*, Docket No. C-4640, *supra* note 28; *FTC v. Effen Ads, LLC*, Case No. 2:19-cv-00945 (D. Utah); FTC Press Release, *Operators of Multi-Million Dollar Work-from-Home Scheme Settle FTC Allegations* (Dec. 30, 2019), at <https://www.ftc.gov/news-events/press-releases/2019/12/operators-multi-million-dollar-work-home-scheme-settle-ftc>; *LeanSpa, LLC, et al.*, Case No 3:11-cv-1715 (D. Conn.); FTC Press Release, *U.S. Circuit Court Finds Operator of Affiliate Marketing Network Responsible for Deceptive Third-Party Claims Made for LeanSpa Weight-loss Supplement* (Oct. 4, 2016), at <https://www.ftc.gov/news-events/press-releases/2016/10/us-circuit-court-finds-operator-affiliate-marketing-network>.

³³ FTC Enforcement Policy Statement on Deceptively Formatted Advertisements (Dec. 22, 2015), https://www.ftc.gov/system/files/documents/public_statements/896923/151222_deceptiveenforcement.pdf.

³⁴ *FTC v. Effen Ads, LLC*, Case No. 2:19-cv-00945 (D. Utah); FTC Press Release, *Operators of Multi-Million Dollar Work-from-Home Scheme Settle FTC Allegations* (Dec. 30, 2019), at <https://www.ftc.gov/news-events/press-releases/2019/12/operators-multi-million-dollar-work-home-scheme-settle-ftc>.

³⁵ FTC Complaint, *FTC v. Effen Ads, LLC*, Case No. 2:19-cv-00945 (D. Utah), available at <https://www.ftc.gov/system/files/documents/cases/1723202catalystcomplaint.pdf>.

³⁶ *Id.*

³⁷ *Id.*

³⁸ The advertisement or website must be viewed as a whole, including visual and aural elements. The net impression of the advertisement is controlling. FTC Policy Statement on Deception (Oct. 14, 1983), available at https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf [hereinafter “FTC Deception Policy Statement”]; *Pfizer Inc.*, 81 F.T.C. 23, 58 (1972); *Beneficial Corp. v. FTC*, 542 F.2d 611, 617 (3d Cir. 1976).

³⁹ For example, a Pew Research Center survey conducted in 2005 reported that 45% of search engine users said they would stop using a search engine if it did not make it clear that some results were paid or sponsored. Pew Internet & Am. Life Project, *Search Engine Users: Internet searchers are confident, satisfied and trusting – but they are also unaware and naïve*, at 20 (Jan. 23, 2005), <http://www.pewinternet.org/Reports/2005/Search-Engine-Users/1-Summary-of-Findings.aspx>. See also FTC, *Soliciting and Paying for Online Reviews: A Guide for Marketers* (January 2022), at <https://www.ftc.gov/business-guidance/resources/soliciting-paying-online-reviews-guide-marketers>.

⁴⁰ See CMA Online Choice Architecture Paper, at 37 (“[A]cademic research shows that across several contexts (and particularly online), items appearing (ranked) at the top of the list are more likely to be clicked and chosen. The effectiveness of ranking shares many psychological mechanisms with defaults...including reduced effort, salience, and beliefs about quality or relevance, such that items appearing higher perform better.”)

⁴¹ FTC Enforcement Policy Statement on Deceptively Formatted Advertisements (Dec. 22, 2015), available at https://www.ftc.gov/system/files/documents/public_statements/896923/151222_deceptiveenforcement.pdf.

⁴² See CMA Online Choice Architecture Paper, at 38 (“Third-party businesses may therefore be unable to improve their search ranking or may find it difficult to draw customers away from the incumbent.”).

⁴³ *In the Matter of LendEDU, et al.*, Docket No. C-4719; FTC Press Release, *Operators of Comparison Shopping Website Agree to Settle FTC Charges Alleging Deceptive Rankings of Financial Products and Fake Reviews* (Feb. 3, 2020), at <https://www.ftc.gov/news-events/press-releases/2020/02/operators-comparison-shopping-website-agree-settle-ftc-charges>.

⁴⁴ FTC Complaint, *In the Matter of LendEDU, et al.*, Docket No. C-4719, available at https://www.ftc.gov/system/files/documents/cases/c-4719_182_3180_lendedu_complaint.pdf.

⁴⁵ *Id.*

⁴⁶ *Id.*

⁴⁷ *Id.*

⁴⁸ See FTC Policy Statement on Deception, *supra* note 38; FTC Enforcement Policy Statement on Deceptively Formatted Advertisements, *supra* note 33.

⁴⁹ See FTC Deception Policy Statement, at 4 (“Depending on the circumstances, accurate information in the text may not remedy a false headline because reasonable consumers may glance only at the headline. Written disclosures or fine print may be insufficient to correct a misleading representation.”); FTC, *Featuring Online Customer Reviews: A Guide for Platforms* (January 2022), at <https://www.ftc.gov/business-guidance/resources/featuring-online-customer-reviews-guide-platforms>.

⁵⁰ See Statement in Regard to Advertisements That Appear in Feature Article Format, FTC Release, (Nov. 28, 1967) (In some instances, “the format of [an] advertisement may so exactly duplicate a news or feature article as to render the caption ‘ADVERTISEMENT’ meaningless and incapable of curing the deception.”). See also FTC, *Blurred Lines: An Exploration of Consumers’ Advertising Recognition in the Contexts of Search Engines and Native Advertising: A Federal Trade Commission Staff Report* (Dec. 2017), at 22, available at https://www.ftc.gov/system/files/documents/reports/blurred-lines-exploration-consumers-advertising-recognition-contexts-search-engines-native/p164504_ftc_staff_report_re_digital_advertising_and_appendices.pdf [hereinafter “Blurred Lines FTC Staff Report”] (“The Gear Patrol and Chicago Tribune conditions appeared to have fewer indicia separate and apart from the disclosure that they were advertisements. For both these native ads, assessed ad recognition was low to begin with, and seemed to improve very little with the improved disclosures.”).

⁵¹ See Blurred Lines FTC Staff Report, at 1 (“In other words, consumers should be able to recognize an ad as an ad. If a separate disclosure is necessary to make that happen, the disclosure should be made in a way that ensures consumers can read, process, and understand it.”). See also FTC Deception Policy Statement, at 4 (design practices that operate to direct consumers’ attention away from qualifying disclosures or other material information are deceptive); CMA Online Choice Architecture Paper, at 38 (“[T]here is some evidence from research that these types of disclosures are not always well understood or used by consumers and it may be necessary to construct them carefully.”).

⁵² Dark Patterns Workshop Transcript, at 8 (“Some dark patterns are information-hiding, meaning they delay or hide important information from users.”). *See, e.g., In the Matter of Nat’l Payment Network, Inc.*, Docket No. 132 3285 (charging NPN with deceptively pitching consumers an auto payment program it claimed would save consumers money but failing to disclose that the significant fees it charged for the service often cancelled out any actual savings); FTC Press Release, *FTC, Multiple Law Enforcement Partners Announce Crackdown on Deception, Fraud in Auto Sales, Financing and Leasing* (March 26, 2015), at <https://www.ftc.gov/news-events/news/press-releases/2015/03/ftc-multiple-law-enforcement-partners-announce-crackdown-deception-fraud-auto-sales-financing>; *FTC v. Match Group, Inc.*, Case No. 3:19-02281 (N.D. Texas) (charging the operators of Match.com with deceptively inducing consumers to subscribe to the dating service by promising them a free six-month subscription without adequately disclosing that consumers would need to comply with additional terms before the company would honor the guarantee); FTC Press Release, *FTC Sues Owner of Online Dating Service Match.com for Using Fake Love Interest Ads To Trick Consumers into Paying for a Match.com Subscription* (Sept. 25, 2019), at <https://www.ftc.gov/news-events/news/press-releases/2019/09/ftc-sues-owner-online-dating-service-matchcom-using-fake-love-interest-ads-trick-consumers-paying#:~:text=The%20%20FTC%20alleges%20consumers%20often%20were%20unaware%20they,the%20free%20six%20months%20%20of%20service%20they%20expected.>

⁵³ *FTC v. LendingClub Corp.*, Case No. 3:18-cv-02454 (N.D. Cal.); FTC Press Release, *LendingClub Agrees to Pay \$18 Million to Settle FTC Charges* (July 14, 2021), at <https://www.ftc.gov/news-events/press-releases/2021/07/lendingclub-agrees-pay-18-million-settle-ftc-charges>.

⁵⁴ FTC Complaint, *FTC v. LendingClub Corp.*, Case No. 3:18-cv-02454 (N.D. Cal.), available at https://www.ftc.gov/system/files/documents/cases/lendingclub_corporation_first_amended_complaint.pdf.

⁵⁵ A tooltip button is an icon, image, or other graphical element that, when a user interacts with it or their cursor is positioned over it, prompts a textbox displaying relevant information to appear. In other words, such a mouse-over or hover-over causes a pop-up.

⁵⁶ FTC Complaint against *LendingClub Corp.*, *supra* note 54.

⁵⁷ *Id.*

⁵⁸ *Id.*

⁵⁹ Dark Patterns Workshop Transcript, at 7, 8, 68. *See also* Mary W. Sullivan, Federal Trade Commission, Bureau of Economics, *Economic Analysis of Hotel Resort Fees* (January 2017), at 36, available at https://www.ftc.gov/system/files/documents/reports/economic-analysis-hotel-resort-fees/p115503_hotel_resort_fees_economic_issues_paper.pdf (“This analysis finds that separating mandatory resort fees from posted room rates without first disclosing the total price is likely to harm consumers by increasing the search costs and cognitive costs of finding and choosing hotel accommodations.”); CMA Online Choice Architecture Paper, at 29 (“Since consumers often focus on headline prices, showing the total price in increments – ‘dripped’ through the purchase process – can affect consumer behaviour. Additional fees, compulsory or optional, may be obfuscated and therefore not noticed.”).

⁶⁰ Dark Patterns Workshop Transcript, at 80. *See also* CMA Online Choice Architecture Paper, at 30 (“Once a

consumer is psychologically committed to a purchase or course of action, abandoning it may cause feelings of uncertainty, dissatisfaction and cognitive dissonance. Businesses may also use drip pricing to draw consumers in on a low headline rate, then rely on the extra effort that would be required for them to go back and find an alternative, such that consumers accept the price increasing later in the purchase process. These mechanisms draw on several behavioural biases, including anchoring (people tend to anchor on initial price information and fail to fully adjust their view of the price as additional fees are revealed), sunk cost fallacy (people tend to continue with a process if they have invested time or effort, such as exploring a product or providing their personal details), and the endowment effect (people tend to place a higher value on objects they own, or have imagined owning).”).

⁶¹ Dark Patterns Workshop Transcript, at 7; Blake et al., *Price Salience and Consumer Choice* (2020).

⁶² See, e.g., CMA Online Choice Architecture Paper, at 30.

⁶³ Dark Patterns Workshop Transcript, at 80. See also FTC Press Release, *FTC Warns Hotel Operators that Price Quotes that Exclude 'Resort Fees' and Other Mandatory Surcharges May Be Deceptive*, (Nov. 28, 2012), at <https://www.ftc.gov/news-events/news/press-releases/2012/11/ftc-warns-hotel-operators-price-quotes-exclude-resort-fees-other-mandatory-surcharges-may-be>; *Economic Analysis of Hotel Resort Fees*, supra note 59 (“Hotels could eliminate these costs to consumers by including the resort fee in the advertised price. They could still bundle the same resort services with the room and charge the same total price. They could also list the components of the total price separately, as long as the total price is the most prominently disclosed price.”).

⁶⁴ See *FTC v. Universal City Nissan, Inc.*, et al., (C.D. Cal.); FTC Press Release, *Los Angeles-Based Sage Auto Group Will Pay \$3.6 Million to Settle FTC Charges* (March 14, 2017), at <https://www.ftc.gov/news-events/news/press-releases/2017/03/los-angeles-based-sage-auto-group-will-pay-36-million-settle-ftc-charges>.

⁶⁵ The Equal Credit Opportunity Act, or ECOA, prohibits credit discrimination on the basis of race, color, religion, national origin, sex, marital status, age, or because you get public assistance. 15 U.S.C. §§ 1691-1691f.

⁶⁶ See, e.g., *FTC v. Liberty Chevrolet, Inc. d/b/a Bronx Honda*, Case No. 1:20-cv-03945-PAE (S.D.N.Y.) (According to the FTC complaint, defendants charged higher financing markups and fees to African-American and Hispanic customers than to similarly situated non-Hispanic white consumers. In addition, the FTC charged defendants caused consumers to pay substantially more than they expected, failing to honor the advertised sales price and inflating the cost through a variety of methods.); FTC Press Release, *Auto Dealership Bronx Honda, General Manager to Pay \$1.5 Million to Settle FTC Charges They Discriminated Against African-American, Hispanic Car Buyers* (May 27, 2020), at <https://www.ftc.gov/news-events/press-releases/2020/05/bronx-honda-to-pay-over-1-million-to-settle-charges>; *FTC and The State of Illinois v. North American Automotive Services, Inc.*, et al., Case No. 1:22-cv-01690 (N.D. Ill.); FTC Press Release, *FTC Takes Action Against Multistate Auto Dealer Napleton for Sneaking Illegal Junk Fees onto Bills and Discriminating Against Black Consumers* (Apr. 1, 2022), at <https://www.ftc.gov/news-events/news/press-releases/2022/04/ftc-takes-action-against-multistate-auto-dealer-napleton-sneaking-illegal-junk-fees-bills>.

⁶⁷ When a representation or sales practice targets a specific audience, such as children, older adults, or the terminally ill, “ordinary consumers” for purposes of Section 5 of the FTC Act includes reasonable members of the targeted group. FTC Deception Policy Statement.

⁶⁸ See Dark Patterns Workshop Transcript, at 50, 74.

⁶⁹ See Blurred Lines FTC Staff Report at 4, 20.

⁷⁰ The Children’s Online Privacy Protection Act, or COPPA, requires companies to protect children’s privacy and safety online, including by getting parental consent before collecting some types of information from kids under 13. 15 U.S.C. §§ 6501–6505.

⁷¹ Enforcement Policy Statement Regarding Negative Option Marketing, 86 Fed. Reg 60822, *supra* note 4.

⁷² See EU Dark Patterns Report, at 91.

⁷³ Dark Patterns Workshop Transcript, at 36.

⁷⁴ Specifically, while Apple and Google included prompts for parents to enter their password and authorize an initial purchase, the FTC alleged they did not disclose that authorizing a single purchase also authorized unlimited purchases for a limited time thereafter (15 minutes for Apple and 30 minutes for Google). *In the Matter of Apple Inc.*, Docket No. C-4444; FTC Press Release, *Apple Inc. Will Provide Full Consumer Refunds of At Least \$32.5 Million to Settle FTC Complaint It Charged for Kids’ In-App Purchases Without Parental Consent* (Jan. 15, 2014), at <https://www.ftc.gov/news-events/press-releases/2014/01/apple-inc-will-provide-full-consumer-refunds-least-325-million>; *In the Matter of Google Inc.*, Docket No. C-4499; FTC Press Release, *Google to Refund Consumers at Least \$19 Million to Settle FTC Complaint It Unlawfully Billed Parents for Children’s Unauthorized In-App Charges* (Sept. 4, 2014), at <https://www.ftc.gov/news-events/press-releases/2014/09/google-refund-consumers-least-19-million-settle-ftc-complaint-it>.

⁷⁵ *FTC v. Amazon.com Inc.*, Case No. 2:14-cv-01038 (W.D. Wash.); FTC Press Release, *Federal Court Finds Amazon Liable for Billing Parents for Children’s Unauthorized In-App Charges* (Apr. 27, 2016), at <https://www.ftc.gov/news-events/press-releases/2016/04/federal-court-finds-amazon-liable-billing-parents-childrens>.

⁷⁶ FTC Complaint, *FTC v. Amazon.com Inc.*, Case No. 2:14-cv-01038 (W.D. Wash.), available at <https://www.ftc.gov/system/files/documents/cases/140710amazoncmpt1.pdf>.

⁷⁷ Order Granting Amazon’s Motion for Partial Summary Judgment and Granting the FTC’s Motion for Summary Judgment, *FTC v. Amazon.com Inc.*, Case No. 2:14-cv-01038 (W.D. Wash.), at 3, available at <https://www.ftc.gov/system/files/documents/cases/160427amazonorder.pdf>.

⁷⁸ FTC Complaint against *Amazon.com Inc.*, *supra* note 76.

⁷⁹ FTC Press Release, *FTC, Amazon to Withdraw Appeals, Paving Way for Consumer Refunds Related to Children’s Unauthorized In-App Charges* (Apr. 4, 2017), at <https://www.ftc.gov/news-events/press-releases/2017/04/ftc-amazon-withdraw-appeals-paving-way-consumer-refunds-related>; FTC Press Release, *Refunds Now Available from Amazon for Unauthorized In-App Purchases* (May 30, 2017), at <https://www.ftc.gov/news-events/news/press-releases/2017/05/refunds-now-available-amazon-unauthorized-app-purchases>.

⁸⁰ Dark Patterns Workshop Transcript, at 26-27; Luguri & Strahilevitz, *Shining a Light on Dark Patterns*, *supra* note 8.

⁸¹ Dark Patterns Workshop Transcript, at 28; Luguri & Strahilevitz, *Shining a Light on Dark Patterns*, *supra* note 8.

⁸² FTC, “Negative Options: A Workshop Analyzing Negative Option Marketing,” at <https://www.ftc.gov/news-events/events/2007/01/negative-options-workshop-analyzing-negative-option-marketing>.

⁸³ A negative option is a term or condition under which the seller may interpret the consumer’s silence or failure to take action to reject a good or to cancel an agreement as acceptance or continuing acceptance of the offer. A common example of a negative option is a company offering a free trial period, followed by a recurring subscription charge if the consumer doesn’t cancel the subscription before the free trial runs out. Other examples include automatic renewals, continuity plans, fee-to-pay conversions, and prenotification plans. *See* Enforcement Policy Statement Regarding Negative Option Marketing, 86 Fed. Reg 60822, *supra* note 4. *See also* Telemarketing Sales Rule, 16 U.S.C. § 310.2(w) (“Negative option feature means, in an offer or agreement to sell or provide any goods or services, a provision under which the customer's silence or failure to take an affirmative action to reject goods or services or to cancel the agreement is interpreted by the seller as acceptance of the offer.”).

⁸⁴ The staff report covered topics such as disclosure of material terms, including their appearance and timing; obtaining consumers' affirmative consent; and appropriate cancellation procedures. FTC, *Negative Options: A Report by the Staff of the FTC's Division of Enforcement* (January 2009), available at <https://www.ftc.gov/sites/default/files/documents/reports/negative-options-federal-trade-commission-workshop-analyzing-negative-option-marketing-report-staff/p064202negativeoptionreport.pdf>.

⁸⁵ Rule on the Use of Prenotification Negative Option Plans, 16 CFR Part 425.

⁸⁶ The Restore Online Shoppers’ Confidence Act (“ROSCA”), 15 U.S.C. §§ 8401-8405.

⁸⁷ *Id.*

⁸⁸ *See e.g.*, *FTC v. AdoreMe, Inc.*, Case No. 1:17-cv-09083 (S.D.N.Y.); FTC Press Release, *Online Lingerie Marketer Prohibited from Deceiving Shoppers About Negative-Option Programs* (Nov 21, 2017), at <https://www.ftc.gov/news-events/news/press-releases/2017/11/online-lingerie-marketer-prohibited-deceiving-shoppers-about-negative-option-programs>; *In re: UrthBox, Inc.*, Docket No. C-4676; FTC Press Release, *UrthBox Settles FTC Charges Related to Compensated Online Reviews and “Free” Trial Offer* (April 3, 2019), at <https://www.ftc.gov/news-events/news/press-releases/2019/04/urthbox-settles-ftc-charges-related-compensated-online-reviews-free-trial-offer>; *U.S. v MyLife.com, Inc.*, Case No. 20-cv-6692 (C.D. Cal.); FTC Press Release, *FTC, DOJ Obtain Ban on Negative Option Marketing and \$21 Million for Consumers Deceived by Background Report Provider MyLife* (Dec.16, 2021), at <https://www.ftc.gov/news-events/news/press-releases/2021/12/ftc-doj-obtain-ban-negative-option-marketing-21-million-consumers-deceived-background-report>.

⁸⁹ *FTC v. Health Formulas, LLC, also d/b/a Simple Pure Nutrition*, Case No. 2:14-cv-1649-RFB-GWF (D. Nev.); FTC Press Release, *Marketers of Simple Pure Supplements Settle FTC Court Action* (May 3, 2016), at <https://www.ftc.gov/news-events/press-releases/2016/05/marketers-simple-pure-supplements-settle-ftc-court-action>.

⁹⁰ FTC Complaint, *FTC v. Health Formulas, LLC, also d/b/a Simple Pure Nutrition*, Case No. 2:14-cv-1649-RFB-GWF (D. Nev.), available at <https://www.ftc.gov/system/files/documents/cases/1604simplepurecmpt.pdf>.

⁹¹ See Dark Patterns Workshop Transcript, at 4; Helena Vieria, *Bad choice design can be particularly harmful for less educated individuals* (January 31, 2018), at <https://blogs.lse.ac.uk/businessreview/2018/01/31/bad-choice-design-can-be-particularly-harmful-for-less-educated-individuals/> (Studying consumers who had been enrolled in fraudulent subscription services, researchers found that cancelling subscriptions by default increased cancellations to 99.8 per cent—63.4 percentage points higher than requiring consumers to actively cancel in response to a complex, five-paragraph letter). In addition to costing consumers money, companies with overly-difficult cancellation procedures may also harm competition; such unlawful customer-retention practices can prevent consumers from being able to switch to other providers in the market who may better fit their interests or offer better price terms. See, e.g., EU Dark Patterns Report, at 92; CMA Online Choice Architecture Paper, at 32.

⁹² *FTC v. Age of Learning, Inc., also d/b/a ABCmouse and ABCmouse.com*, Case No. 2:20-cv-07996 (C.D. Cal.); FTC Press Release, *Children’s Online Learning Program ABCmouse to Pay \$10 Million to Settle FTC Charges of Illegal Marketing and Billing Practices* (Sept. 2, 2020), at <https://www.ftc.gov/news-events/press-releases/2020/09/childrens-online-learning-program-abcmouse-pay-10-million-settle>.

⁹³ FTC Complaint, *FTC v. Age of Learning, Inc., also d/b/a ABCmouse and ABCmouse.com*, Case No. 2:20-cv-07996 (C.D. Cal.), available at <https://www.ftc.gov/system/files/documents/cases/1723086abcmousecomplaint.pdf>.

⁹⁴ *Id.*

⁹⁵ *Id.*

⁹⁶ *Id.*

⁹⁷ *Id.*

⁹⁸ Dark Patterns Workshop Transcript, at 6 (“For example, trying to cancel a premium subscription when you’re called to call a phone line during working hours, to then have a rep try and talk you out of it for 10 minutes before you’re finally allowed to leave.”).

⁹⁹ ROSCA requires sellers of goods and services over the internet using a negative option feature to provide a simple mechanism for the consumer to stop recurring charges. 15 U.S.C. § 8403(3).

¹⁰⁰ Beyond the general guidance in part III, the FTC has given additional guidance in specific contexts, such as a negative option. See, e.g., FTC, Enforcement Policy Statement Regarding Negative Option Marketing, 86 Fed. Reg. 60822 at 60825 (Nov. 4, 2021) (“To attain express informed consent, the negative option seller should obtain the consumer’s acceptance of the negative option feature offer separately from any other portion of the entire transaction; not include any information that interferes with, detracts from, contradicts, or otherwise undermines the ability of consumers to provide their express informed consent to the negative option feature; obtain the consumer’s unambiguously affirmative consent to the negative option feature; obtain the consumer’s unambiguously affirmative consent to the entire transaction; and be able to verify the consumer’s consent.”).

¹⁰¹ See, e.g., definition of “Express, Informed Consent” in the FTC’s Orders against *Apple Inc.*, available at <https://www.ftc.gov/sites/default/files/documents/cases/140115appleagree.pdf>, and *Google*, available at <https://www.ftc.gov/system/files/documents/cases/141205googleplaydo.pdf>.

¹⁰² See *FTC v. Health Formulas, LLC*, Case No. 2:14-CV-01649-RFB, 2015 WL 2130504, at *17 (D. Nev. May 6, 2015) (inadequate disclosures “cannot serve as the basis for customers’ express, informed consent.”).

¹⁰³ Dark Patterns Workshop Transcript, at 47 (“All your accounts are connected to that [cell phone] device. And it presumes that there’s a single user. But in many communities, cell phones are a luxury commodity. They’re shared among individuals. There’s no way to protect individual users on a cell phone. So we have this bias in the way that we build these technologies.”).

¹⁰⁴ Enforcement Policy Statement Regarding Negative Option Marketing, 86 Fed. Reg 60822 at 60826, *supra* note 4.

¹⁰⁵ *Id.*

¹⁰⁶ See Dark Patterns Workshop Transcript, at 11 (“There’s no excuse for not allowing users to leave a service in the same location they signed up for it.”)

¹⁰⁷ Enforcement Policy Statement Regarding Negative Option Marketing, 86 Fed. Reg 60822 at 60826, *supra* note 4.

¹⁰⁸ See *FTC v. RagingBull.com, LLC*, Case No. 1:20-cv--3538 (D. Md.); FTC Press Release, *Online Investment Site to Pay More Than \$2.4 Million for Bogus Stock Earnings Claims and Hard-to-Cancel Subscription Charges* (March 8, 2022), at <https://www.ftc.gov/news-events/news/press-releases/2022/03/online-investment-site-pay-more-24-million-bogus-stock-earnings-claims-hard-cancel-subscription>.

¹⁰⁹ See Dark Patterns Workshop Transcript, at 32; IDAC Public Comment, *supra* note 12, at 1 (“User interfaces for opting out of data sharing are often impossible to navigate, leaving users either unaware of their privacy options or frustrated in their effort to exercise their rights.”).

¹¹⁰ See Dark Patterns Workshop Transcript, at 32, 45. One panelist asserted that a dark pattern that subverts consumer privacy preferences also “undermines competition by enabling an incumbent online service to extract valuable consumer data and entrench their market dominance.” *Id.* at 32.

¹¹¹ *Id.* at 8, 31-32, 38-39, 69; See also Transcript of FTC Hr’g, *The FTC’s Approach to Consumer Privacy* (Apr. 10, 2019), at 129, available at https://www.ftc.gov/system/files/documents/public_events/1418273/ftc_hearings_session_12_transcript_day_2_4-10-19.pdf (remarks of FTC Commissioner Rebecca Kelly Slaughter, describing privacy consent as illusory because consumers often have no choice other than to consent in order to reach digital services that have become necessary for participation in contemporary society, and even where it appears consumers gave valid consent, that agreement might be a product of manipulative dark patterns); Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 Wash. U. L. Rev. 1461, 1489 (2019) (describing several examples of what the authors call “coerced consent”—including when a user does not have the option to decline but only to accept “later,” or a user interface that words the option to decline in such a way as to shame the user into compliance—which at scale, the authors argue, can accumulate to deplete a user’s resolve with respect to their privacy choices).

¹¹² *Id.* at 8. *See also* EU Dark Patterns Report, at 94 (“For instance, the results showed that nudging (highlighting “Accept” buttons or pre-selecting checkboxes) substantially affects people’s acceptance of cookies, providing clear evidence for the interference of such dark patterns with people’s consent decisions.”) (citing Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T., *(Un) informed consent: Studying GDPR consent notices in the field* (Nov. 2019); DuckDuckGo, Public Comment Submitted to FTC on Dark Patterns Issues, FTC-2021-0019-0103, at 2, available at <https://www.regulations.gov/comment/FTC-2021-0019-0103>; Damien Snyder, Public Comment Submitted to FTC on Dark Patterns Issues, FTC-2021-0019-0001, available at <https://www.regulations.gov/comment/FTC-2021-0019-0046>).

¹¹³ Dark Patterns Workshop Transcript, at 8.

¹¹⁴ *Id.* at 33 (“So I’m of the opinion that the present mechanism of hitting ‘I Accept’ with no attempt to actually inform you in a user-friendly way of what you’re consenting to is potentially inherently manipulative.”). *See also* EU Dark Patterns Report, at 21 (“Individuals do not give meaningful and conscious consent to the use of their data and their behaviours are easily influenced through environmental cues, such as defaults, and the design of web environments owing to pervasive reliance on heuristics and social norms (see for instance Acquisti et al., 2015 or Richards & Hartzog, 2019).”).

¹¹⁵ Dark Patterns Workshop Transcript, at 32-33, 39. *See also* EU Dark Patterns Report, at 60 (“Overall, an important concern for mystery shoppers was not knowing for sure how the websites/apps used their personal data, and with which other companies they would share it. They noted that some websites/apps were asking them for a lot more personal data than what was considered useful for the functioning of the service (e.g., gender, birthdate, astrological sign, etc).”); DuckDuckGo Public Comment, *supra* note 112, at 3; Digital Democracy Public Comment, *supra* note 15, at 18.

¹¹⁶ Dark Patterns Workshop Transcript, at 32.

¹¹⁷ *Id.* at 32 (“cell phone numbers are kind of the new social security number in some ways because we don’t change them . . . it’s another way they can identify you.”); *id.* at 67 (describing as a dark pattern the FTC’s allegation that Facebook collected phone numbers purportedly to enable two-factor authentication, but also used the information to target ads).

¹¹⁸ *Id.* at 39.

¹¹⁹ *Id.* at 39 (“And location data is extremely valuable and can reveal so many things about you, such as where you live, where you work, where you spend your nights. It can reveal your political affiliation, your religious affiliation, your sexual orientation, and so on.”); *see also* Jon Keegan & Alfred Ng, *There’s a Multibillion-Dollar Market for Your Phone’s Location Data*, The Markup (Sept. 30, 2021), available at <https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data> (explaining that a consumer’s location data can be sold repeatedly in the location data marketplace, such as to aggregators that resell the data to multiple sources, to location intelligence firms that use the raw data to analyze foot traffic in retail locations and demographics of visitors, and to hedge funds looking for insights into the popularity of certain stores).

¹²⁰ *FTC v. Kochava, Inc.*, Case No. 2:22-cv-377 (D. Idaho); FTC Press Release, *FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations* (Aug. 29, 2022), at <https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other>.

¹²¹ FTC Complaint, *FTC v. Kochava, Inc.*, Case No. 2:22-cv-377 (D. Idaho), available at https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf.

¹²² FTC Staff Report, *What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers* (Oct. 21, 2021), available at https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf [hereinafter FTC Staff Report—What ISPs Know About You].

¹²³ FTC Staff Report—What ISPs Know About You, at 39.

¹²⁴ *Id.* at 39. *See also* Dark Patterns Workshop Transcript, at 33 (“And I’d really like to see solutions that go further than just giving us kind of new looks on existing interfaces, such as, one of the things we look at is whether the Accept button is highlighted in advance.”).

¹²⁵ FTC Staff Report—What ISPs Know About You, at 39-40.

¹²⁶ *Id.* at 40-41. *See also* FTC Complaint, *PayPal, Inc.*, Docket No. C-4651, available at https://www.ftc.gov/system/files/documents/cases/1623102_c-4651_paypal_venmo_complaint_final.pdf (alleging that where two different settings related to the public visibility of users’ transactions on Venmo, Respondent failed to disclose, or failed to disclose adequately, that toggling off one setting did not ensure that future transactions would be visible only to a more limited audience (*i.e.*, only to friends or to other participants in the transaction)).

¹²⁷ FTC Staff Report—What ISPs Know About You, at 41.

¹²⁸ *FTC v. VIZIO, Inc. and VIZIO Inscape Servs., LLC*, (D. N.J.); FTC Press Release, *Vizio to Pay \$2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions Without Users’ Consent* (Feb. 6, 2017), at <https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it>.

¹²⁹ FTC Complaint, *FTC v. VIZIO, Inc. and VIZIO Inscape Servs., LLC*, (D. N.J.), available at https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf.

¹³⁰ *Id.*

¹³¹ *Id.*

¹³² *FTC v. Sunkey Publ’g, Inc. et. al*, Case No. 3:18-cv-01444-HNJ (N.D. Alabama); FTC Press Release, *FTC Takes Action against the Operators of Copycat Military Websites* (Sept. 6, 2018), at <https://www.ftc.gov/news-events/press-releases/2018/09/ftc-takes-action-against-operators-copycat-military-websites>.

¹³³ FTC Complaint, *FTC v. Sunkey Publ'g, Inc. et. al*, Case No. 3:18-cv-01444-HNJ (N.D. Alabama), available at https://www.ftc.gov/system/files/documents/cases/sunkey_filed_complaint.pdf.

¹³⁴ *Id.*

¹³⁵ *FTC v. Day Pacer LLC, f/k/a College Criteria LLC, also d/b/a Edutrek*, Case No. 1:19-cv-01984 (N.D. Ill.); FTC Press Release, *FTC Charges Telemarketing Operation with Misleading Job Seekers and Making Millions of Illegal, Unsolicited Calls* (Apr. 12, 2019), at <https://www.ftc.gov/news-events/press-releases/2019/04/ftc-charges-telemarketing-operation-misleading-job-seekers-making>.

¹³⁶ *FTC v. Blue Global and Christopher Kay*, (D. Ariz.); FTC Press Release, *FTC Halts Operation that Unlawfully Shared and Sold Consumers' Sensitive Data* (July 5, 2017), at <https://www.ftc.gov/news-events/press-releases/2017/07/ftc-halts-operation-unlawfully-shared-sold-consumers-sensitive>.

¹³⁷ *FTC v. ITMedia Solutions LLC, et al.*, Case No. 2:16-cv-09483 (C.D. Cal.); FTC Press Release, *Lead Generator that Deceptively Solicited Loan Applications from Millions of Consumers and Indiscriminately Shared Sensitive Info Agrees to Pay \$1.5 Million FTC Penalty* (Jan. 7, 2022), at <https://www.ftc.gov/news-events/press-releases/2022/01/lead-generator-deceptively-solicited-loan-applications-millions>.