NAI
PRIVACY, ACCOUNTABILITY & TRUST

APRIL 2022

Best Practices for User Choice and Transparency

TABLE OF CONTENTS

1. Introduction

The Network Advertising Initiative ("NAI") is the premier self-regulatory organization for the advertising technology industry. Throughout its twenty-year history, the NAI has been at the forefront of promoting consumer privacy through transparency and user choice. As the digital ecosystem has evolved, the NAI has continued to champion best practices that reflect this commitment, both through the Code of Conduct ("Code"), and through guidance documents and resources for members and the industry at large.

This Guidance, developed by NAI legal and policy staff in consultation with representatives from member companies, is intended to help member companies better understand the practice of dark patterns and to implement the highlighted best practices to avoid them. This Guidance has a threefold purpose: to explain consumer choice and transparency obligations under the NAI Code; to examine the current legal environment at the state and federal levels; and to identify best practices and guide companies in maximizing effective and efficient notice and choice mechanisms with respect to collecting consumer data. Certain terms used in state and federal regulation may not line up precisely with terms used in the NAI Code; in those instances, we have noted the appropriate term in the NAI Code that would apply.

The term "dark pattern" was coined in 2010 to refer to "tricks used in websites and apps that make you do things you didn't mean to do, like buying or signing up for something."[1] They are also sometimes referred to as "deceptive patterns" or "manipulative designs." These practices can be dynamic and multifaceted, including a series of tactics and specific design choices in apps and on websites. The NAI and its Code do not specifically address the use of so-called dark patterns by member organizations. However, the goal of this Guidance is to further apply the objectives of the NAI Code, and provide more specific recommendations to encourage companies to maximize transparency and choice for consumers around the collection and use of their data for advertising and marketing purposes.

The legal landscape across the United States is evolving in this area. The states of California and Colorado have adopted prohibitions against the use of dark patterns with respect to consumer data collection under their state data privacy laws. There is also interest in dark patterns on a Federal level; members of Congress reintroduced the Deceptive Experiences to Online Users Reduction (DETOUR) Act in December 2021 to regulate deceptive tactics. The Federal Trade Commission ("FTC") has also indicated an interest in regulating dark patterns under its statutory authority to ban unfair and deceptive acts or practices.

The NAI does not take a position regarding whether the new laws, regulation and enforcement represent a significantly new legal standard. However, we want to make members aware of these developments. More importantly, we remain committed to guiding member companies and the digital advertising ecosystem to provide effective notice and choices to consumers around the collection and use of their personal information.

While this document provides general explanations of certain laws and regulations, it does not constitute legal advice. All NAI members should consult with counsel to determine how the law applies to their specific business activities.

1 Dark Patterns, http://www.darkpatterns.org

2. NAI Code Requirements to Support User Choice and Transparency

Since its inception in 2000, the NAI has championed consumer choice and transparency among its members. In the initial Code of Conduct, the NAI outlined the values that have guided the organization for two decades: privacy, trust, and accountability. The NAI has worked with some of the largest organizations in the digital advertising industry to ensure consumers maintain an ability to control the use of their personal information.[2]

Transparency and choice are fundamental values of the NAI, and this is reflected in the Code. The Code places numerous obligations on member organizations regarding the provision of notice and choice to consumers. The NAI requires clear, conspicuous, and prominent notices on member websites regarding data collection, transfer, and use practices for Tailored Advertising and Ad Delivery and Reporting.[3]

Through the annual compliance review process, NAI staff review members' business practices, consumer choice mechanisms, contractual provisions, marketing materials, and disclosures to ensure that members are in full compliance with the Code. This review process includes technical monitoring of consumer opt-outs. NAI staff meet individually with each member company and discuss Code compliance, outlining any changes that must be made. Compliance staff ensure that members maintain prominent notice on their websites. NAI staff also review member privacy policies and work with members to ensure the language is clear and understandable to consumers.

Since the initial NAI Code of Conduct in 2000, the NAI has provided substantive guidance to member companies regarding robust notice and easily accessible choice mechanisms, including ideal locations for disclosures, links, buttons, or check boxes. During the annual compliance reviews, NAI staff offers feedback to member companies when certain disclosures prove difficult to find or access, when font size or color make text and links difficult to read, or when too many clicks are necessary for users to exercise their choice.

A full list of member transparency obligations may be found in § II.B of the Code. Disclosure obligations include:

- A general description of the member's data collection practices for Tailored Advertising and Ad Delivery and Reporting; the types of data collected and used; and how the data is used, stored, or transferred to a third party;[4]

---

2 Please note the concept of personal information as defined in U.S. laws related to the 2020 NAI Code terms "Personally-Identified Information" and "Device-Identified Information." "Personally-Identified Information" ("PII") is any data linked, or intended to be linked, to an identified individual, including name, address, telephone number, email address, financial account number, and non-publicly available government-issued identifier. *See* Network Advertising Initiative, 2020 NAI Code of Conduct § I.K. "Device-Identified Information" ("DII") is any data that is linked to a particular browser or device if that data is not used, or intended to be used, to directly identify a particular individual. DII includes unique identifiers associated with browsers or devices, such as cookie identifiers or advertising identifiers, and IP addresses, where such data is not linked to PII. *Id.* § I.F.

3 "Tailored Advertising" is the use of previously collected data about an individual, browser, or device to tailor advertising across unaffiliated web domains or applications, or on devices, based on attributes, preferences, interests, or intent linked to or inferred about that user, browser, or device. *Id.* § I.Q. "Ad Delivery and Reporting" ("ADR") is separate and distinct from Tailored Advertising; it refers to the collection or use of data about a browser or device for the purpose of delivering ads or providing advertising-related services. Data collected for ADR later used for Tailored Advertising purposes is treated as Tailored Advertising under the Code. *Id.* § I.A.

4 *Id.* § II.B.1.a.

- A link to or instructions for the Opt-Out Mechanism[5] utilized by the member;[6]
- Disclosure of health-related and political-related interest segments, both standard and custom;[7]
- Contractual requirements for all websites and applications where data is collected or used to provide notice to users, as well as a link to industry consumer choice tools.
- Requirement to provide enhanced notice[8] in any ad unit that relies on previously collected data.

The level of disclosure the Code requires is commensurate with the sensitivity of the data being collected. Under the Code, the collection of any Sensitive Information[9] (as defined by the NAI Code) or the collection of Precise Location Information[10] requires Opt-In Consent.[11] For instance, the NAI's "just in time notice" requires notice prior to the collection of Precise Location Information, recognizing that existing consent mechanisms on mobile devices do not adequately inform consumers about the sharing of their location data. As a result, the NAI requires member companies to ensure that consumers are presented with information about the potential uses of their location data outside of the app before obtaining consent. This also informs consumers about the utility of the data collection, and the available choices with respect to that data.

The NAI requires all member companies that engage in Tailored Advertising to provide additional notice in any ad unit that is informed by previously collected data. This helps ensure that consumers can tell when ads are targeted, learn which companies helped deliver those ads, and exercise their choice to opt out of such targeting.

Additionally, the NAI requires members to engage in consumer education efforts, informing consumers about the choices available to them regarding Tailored Advertising.[12]

These requirements of membership are key to the main principles of the NAI: transparency and accountability, with an eye towards consumer protection and choice. Dark patterns, in contrast, involve obfuscation and a lack of clarity, with the likelihood or outcome of tricking consumers into

5 "Opt-Out Mechanism" is an easy-to-use mechanism by which users may exercise choice to disallow Tailored Advertising with respect to a particular identifier, browser, or device. *Id.* § I.I. Under the definition of Tailored Advertising, an Opt-Out Mechanism allows the consumer to elect to prevent the use of previously collected data from unaffiliated web domains or applications, or on devices, based on attributes, preferences, interests, or intent linked to or inferred about that user, browser, or device for tailored ads.

6 *Id.* § II.B.1.c.

7 *Id.* § II.B.2-3.

8 "Enhanced Notice" is notice of Tailored Advertising data collection and use practices and the NAI-supported choices available to users, in or around advertisements that are informed by such data. Exceptions include when notice is otherwise provided on the web page or application where the ad is served, outside of the publisher's privacy policy or terms of service; and when notice is provided in the application's or device's settings and/or privacy policy and as part of the process of downloading an application to a device, or at the time the application is launched for the first time or during a device's initial setup process, or when the data is first accessed. *Id.* § II.B.8.

9 "Sensitive Information" includes Social Security Numbers or other non-publicly available government-issued identifiers; insurance plan numbers; financial account numbers; information about any past, present, or potential future health or medical conditions or treatment obtained or derived from pharmaceutical prescriptions or medical records; information (including inferences) about sensitive health or medical conditions or treatments; and information (including inferences) about a user's sexual orientation. *Id.* § I.O.

10 "Precise Location Information" is data that describes the precise geographic location of a device derived through any technology that is capable of determining with reasonable specificity the actual location of an individual or device. *Id.* § I.L. For more information, see the NAI's Guidance on Determining Whether Location is Imprecise.

11 "Opt-In Consent" is an easy-to-use mechanism by which users may exercise choice to disallow Tailored Advertising with respect to a particular identifier, browser, or device. *Id.* § I.I. For information about the level of choice members must provide users, see *id.* § II.C.1.

12 *Id.* § II.A.1-2.

making choices they don't necessarily intend. The NAI is concerned about the use of dark patterns that have led to increased attention and regulation. NAI members are well-positioned to avoid these pitfalls. Furthermore, through the annual Compliance Review process, NAI members' practices are assessed by the NAI Compliance team to ensure that members remain compliant with the Code. Members in compliance with the Code will have in place business practices that encourage clear and conspicuous disclosure and notice to consumers, avoiding consumer confusion and ensuring that consumers will not be misled.

3. Legislative and Regulatory Requirements Supporting Transparency and User Choice

There has been a growing trend of legislation and enforcement centered on ensuring user interfaces support transparency and consumer choice. Before assessing the legislative landscape, it may be helpful to identify common touch points with consumers, particularly those that have been the focus of enforcement actions. As technology and design seek to create frictionless consumer experiences, it is important to balance the ease of the user journey with sufficient transparency and choice about data collection and use. Most dark pattern enforcement cases to date have centered around consumer interactions related to point of purchase, upselling and refunds. Based on review of these enforcement actions, analogous activities in the ad-tech ecosystem that are relevant for review include:

- Email or newsletter sign ups or unsubscribes
- Data Collection
    - Personal information
    - Sensitive or precise location data
- Transparent disclosure of data use
- Exercising consumer rights or requests
- Privacy policy accessibility
- Opt in or opt out

When reviewing the legislative history below consider these use cases and how they may apply to your business practices. While various laws define what is considered a dark pattern differently, it is helpful to understand general concepts and techniques used in websites and mobile applications that mislead or manipulate users, obscuring, subverting or impairing consumer autonomy, decision making or choice.

A. The FTC Act – Unfair and Deceptive Acts or Practices

While the U.S. lacks a comprehensive privacy law regulating the use of dark patterns, the Federal Trade Commission Act of 1914 (15 U.S.C. § 41 *et seq.*) includes a provision making "unfair or deceptive acts or practices in or affecting commerce" unlawful (commonly referred to as "Section 5"), effectively regulating dark patterns.[13] The FTC has developed a doctrinal framework for determining if an act or practice is unfair or deceptive, with different analyses for both.

Unfairness
The FTC uses a three-prong test for determining if an act or practice is "unfair." All three elements must be established for the FTC to conclude that any act or practice is unfair. These prongs are:

13 15 U.S.C. § 45(a)(1) (2021).

1. **Whether the practice causes or is likely to cause substantial injury to consumers;**
2. **Whether or not the practice is reasonably avoidable by consumers; and**
3. **Whether the practice is outweighed by countervailing benefits to consumers or to competition.**[14]

For a practice to be reasonably avoidable, the FTC generally trusts that consumers will "survey the available alternatives, choose those that are most desirable, and avoid those that are inadequate or unsatisfactory."[15] However, this consumer choice is predicated on the assumption that the consumer has sufficient information necessary to make an informed decision. This depends both "not just on whether people know the physical steps to take in order to prevent [injury], but also on whether they understand the necessity of actually taking those steps."[16]

Deception
Similar to unfairness, the FTC uses a three-part test to determine if a practice meets its standard of "deception:"

1. **There must be a representation, omission, or practice that is likely to mislead the consumer;**
2. **The representation must be one a reasonable consumer would consider misleading; and**
3. **The representation, omission or practice must be a material one.**[17]

While the FTC has not provided guidance on consent dialogs, looking to its guidance on "deceptive" advertising content can help guide responsible communication to consumers. The FTC considers a reasonable consumer to be a reasonable consumer *to whom the product is targeted*.[18] Importantly, "[a]n interpretation will be presumed reasonable if it is the one the [seller] intended to convey."[19]

For a representation, omission, or practice to be material, it must be one that is likely to affect a consumer's choice of or conduct regarding a product.[20]

Notably, the FTC Act does not consider "intent to deceive" when determining if a commercial practice is in violation of Section 5. Rather, "[i]n determining whether an advertisement, including its format, misleads consumers, the Commission considers the overall 'net impression' it conveys".[21] In doing so, the Commission will look at factors such as (1) overall appearance of the ad placement; (2) similarity of written, spoken, or visual style to non-advertising; and (3) the degree to which it is different from other company content.[22]

14 Fed. Trade Comm'n, A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority (May 2021), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.
15 *Id.*
16 *In re International Harvester Co.*, 104 F.T.C. 1066 (1984).
17 Letter from James C. Miller, Chairman, Federal Trade Commission, to the Hon. John D. Dingell, Member of Congress (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf (hereinafter "Policy Statement on Deception").
18 *Id.*
19 *Id.*
20 Certain categories of information are presumptively material. Express claims, where the seller knew (or should have known) that an ordinary consumer would need omitted information to evaluate the product or service, or that the claim was false, are presumptively material. Claims involving health and safety, "or other areas with which the reasonable consumer would be concerned," are presumptively material.
21 *Enforcement Policy on Deceptively Formatted Advertisements*, Fed. Trade. Comm'n, https://www.ftc.gov/system/files/documents/public_statements/896923/151222deceptiveenforcement.pdf.
22 *Id.*

B. CCPA Regulations and the CPRA

The California Attorney General's office promulgated regulations pursuant to its authority under the California Consumer Privacy Act ("CCPA") (Cal. Civ. Code § 1798.100 *et seq.*) regulating the use of dark patterns with respect to consumer opt-out choices. California law explicitly outlaws the use of opt-out methods "designed with the purpose or [having] the substantial effect of subverting or impairing a consumer's choice to opt-out."[23] Examples include:

- Requiring more steps for submitting a request to opt-out than that business's process for a consumer to opt-in to the sale of personal information after having previously opted out;
- Using confusing language, such as double negatives (*e.g.*, "Don't Not Sell My Personal Information");
- Requiring a consumer to click through or listen to reasons why they should not submit a request to opt-out before confirming their request;
- Requiring a consumer to provide additional personal information that is not necessary to implement the request; and
- Requiring a consumer to search or scroll through the text of a privacy policy or a similar document to locate the mechanism for submitting a request to opt out.[24]

In 2020, California went a step further with the California Privacy Rights Act ("CPRA"), which amends and supplements the CCPA.[25] In addition to explicitly defining dark patterns, the amendment also asserts "consent obtained through dark patterns does not constitute consent."[26]

In complying with California law, companies should pay particular attention to notice requirements, as failing to provide consumers with adequate notice and choice mechanisms could constitute a dark pattern pursuant to the definition codified in the CPRA.[27] For example, adequate opt-out notice to consumers requires the use of plain, straightforward language understandable by a reasonable consumer and accessible to consumers with disabilities. The notice must include a description of the consumer's rights, clear instructions on how to opt-out, etc.[28] As with other data protection regulations, there are heightened responsibilities associated with collecting any sensitive personal information.[29] Further, "[b]usinesses must make the process easy for consumers to execute and must follow a minimal number of steps and a business must not use a method "designed with the purpose or [having] the substantial effect of subverting or impairing" the consumer's choice."[30] These factors must be considered in the design of the consumer opt-out interface in order to obtain consent properly in California.

C. Colorado Privacy Act

Colorado joined California in explicitly defining and outlawing dark patterns when the state passed

23 Cal. Code Regs. tit. 11, § 999.315(h) (2021).
24 *Id.*
25 Cal. Civ. Code § 1798.140.
26 Cal. Civ. Code § 1798.140(h).
27 *Id.*
28 Cal. Code Regs. tit. 11, § 999.315(h) (2021).
29 Cal. Civ. Code § 1798.140(1).
30 *Id.*

the Colorado Privacy Act ("CPA") in 2021.[31] Notably, the CPA adopts the exact definition codified in the CPRA: "'Dark Pattern' means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice."[32]

D. GDPR

While the General Data Protection Regulation ("GDPR") does not explicitly address dark patterns, the regulation's definition of consent provides similar protections and can be analogized to the protections afforded in California and Colorado, and enforcement actions taken by the FTC. According to the GDPR, in order for consent to be valid, it must be "freely given, specific, informed and unambiguous."[33] Consequently, deceptive web and consumer interfaces, and other traditionally recognized "dark patterns" are contrary to this.[34] Pursuant to the GDPR, the CNIL asserts "the fact of using and abusing a strategy to divert attention or dark patterns can lead to invalidating consent."[35] Furthermore, in March 2022, the European Data Protection Board ("EDPB") released a series of its own guidelines on the use of dark patterns in social media platforms, open for public comment.[36]

4. Best Practices

The NAI is committed to providing member companies and the ad tech ecosystem more broadly with guidance for providing effective notice and choice for consumers concerning the use of their personal data. We do not propose these best practices because we have made a determination about the application of a new legal requirement; rather, we agree that dark patterns are problematic and should be avoided. These best practices do not constitute a legal opinion. NAI members should consult with counsel regarding their individual business practices.

A. General Best Practices and Robust User Choice

- **Complete Disclosure:** Clearly include all material terms or conditions when obtaining consumer consent.

- **Accurate Representation of Data Collection, Use, or Sharing:** State terms and conditions about not only the collection of data but its use and sharing in an easily understandable way, not likely to deceive consumers.[37]

    - Avoid employing **"negative options"**—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 an acceptance of the offer."[38]

31 Colo. Rev. Stat.§ 6-1-1303.
32 Colo. Rev. Stat. § 6-1-1303(9).
33 General Data Protection Regulation, No. 2016/679, art. 4(11) 2016 OJ (L 119) (EU).
34 Commission Nationale de l'Informatique et des Libertésf, Shaping Choices in the Digital World (Jan. 2019), https://linc.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf.
35 *Id*.
36 *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognize and avoid them*, European Data Protection Board, https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en (last accessed Apr. 4, 2022).
37 See *In re PayPal, Inc.*, F.T.C. File No. 162 3102 (May 23, 2018); *In re PaymentsMD, LLC*, F.T.C. File. No. 132 3088 (Jan. 27, 2015).
38 16 C.F.R. § 310.2(w).

- Avoid informing consumers that their data is needed for a service to operate when in actuality it is not.[39]

- **Complete Disclosure:** Visually display choices in a way that clearly presents options and alternatives.

  - Make opt-in and opt-out options look **visually similar** and equally accessible.[40]

    - For example, ensure "Accept" and "Cookie Settings" are presented in different, but easy to read text and coloring, clearly delineating different user options.

  - If using **free trials** to enroll consumers, be sure to obtain proper consent before billing and make it easy for consumers to unsubscribe.[41]

  - Use **consistent, readable fonts** and distinct background colors for "Decline" and "Complete Check-Out" options (analogous to opt-outs and consents).[42]

  - Aim to **make the default option the least costly**, and provide information for how to change user preferences in easily readable text (analogous to informed consent).[43]

- **Seamless Cancellations:** Make cancelling subscriptions easy and provide users with complete information about the process.[44]

  - Avoid opt-out processes that are onerous or prompts users to fill out a time-consuming form.

  - Make opt-in and opt-out options look visually similar and equally accessible.[45]

B. Notice and Choice Considerations

For **notice** statements, seek to be as concise as possible, and consider including:

- Clear and easily understandable language that avoids double negatives;
- Language that is as concise as possible, but includes all key elements to enable an informed decision.
- Fully disclosing information about the company's policies and personal data collection practices; and
- Including all material information.[46]

For **choice** options, carefully consider the following:

---

39 See *Fed. Trade Comm'n v. Office Depot, Inc.*, No. 9:19-cv-80431, ECF No. 1 (S.D. Fla. Mar. 27, 2019).
40 See *In re PaymentsMD, LLC*, F.T.C. File No. 132 3088 (Jan. 27, 2015).
41 See *Fed. Trade Comm'n v. NutraClick, LLC*, No. 2:20-cv-08612, ECF No. 1 (Sept. 21, 2021); *Fed. Trade Comm'n v. Age of Learning, Inc.*, No. 2:20-cv-7996, ECF No. 1 (C.D. Cal. Sept. 1, 2020).
42 First Am. Compl. at 5, *Fed. Trade Comm'n v. AH Media, LLC*, No. 19-cv-04022-JD, ECF No. 74 (N.D. Cal. Oct. 23, 2019).
43 See *Fed. Trade Comm'n v. AMG Capital Management*, 910 F.3d 417 (9th Cir. 2018).
44 See *Fed. Trade Comm'n v. NutraClick, LLC*, No. 2:20-cv-08612, ECF No. 1 (Sept. 21, 2021).
45 See *In re PaymentsMD, LLC*, F.T.C. File No.132 3088 (Jan. 27, 2015).
46 See Cal. Code Regs. tit. 11, § 999.306 (2021).

- **Ease of Choice:** Ideally, following clear disclosure, consumers should be provided an opportunity to make a decision easily. This includes not having to read through lengthy privacy policies or similar documents.

- **"Take-It-or-Leave-It" Options:** Though sometimes necessary, consumers are often frustrated by "take-it-or-leave-it" style choices. In circumstances where a product or service is 100% ad supported, and the site or service relies on data-driven advertising, then there are legal requirements that should be considered (*e.g.*, state laws in California and Virginia).

- **Pressure in Language:** Do not use "trick language" to influence consent; do not use manipulative strategies to compel users to select options that are not in their best interests; do not require the collection of personal information that is not necessary to perform choice.

- **Limitations of Choice Mechanisms:** Often, in situations where a user deletes cookies, or starts browsing on a new or unrecognized device or with a new IP address, previously selected privacy settings may be lost or reset, overriding the user's choices regarding data sharing. Where feasible, companies that are aware of this situation should notify users and provide them an opportunity to reestablish their privacy settings.

Things to Avoid When Drafting Notice and Choice Requests

- Do not require more steps for submitting a request to opt-out than that business's process for a consumer to opt-in to the sale of personal information after having previously opted out;

- Do not use confusing language, such as double negatives (*e.g.*, "Don't Not Sell My Personal Information");

- Do not require a consumer to click through or listen to reasons why they should not submit a request to opt-out before confirming their request;

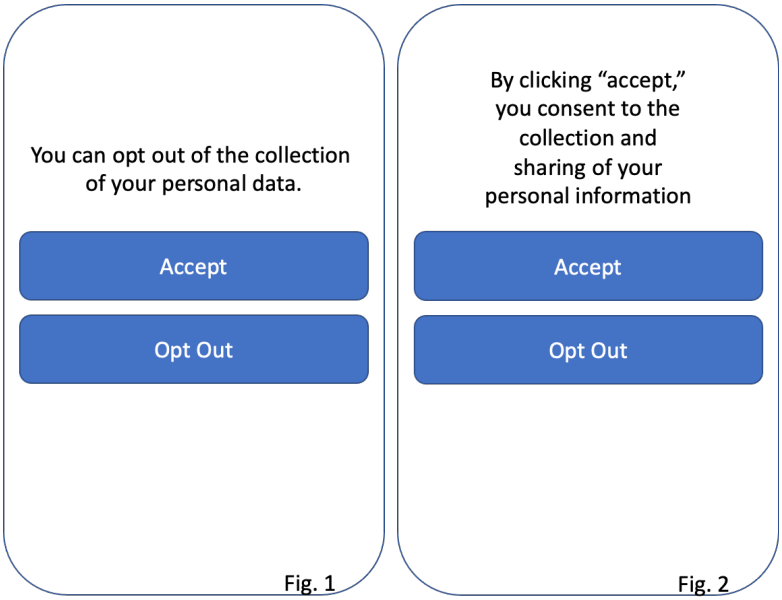
- Do not require a consumer provide personal information that is not necessary to implement the request; and

- Do not require a consumer search or scroll through the text of a privacy policy or a similar document to locate the mechanism for submitting a request to opt out.[47]

C. Considerations for Designing a User Interface

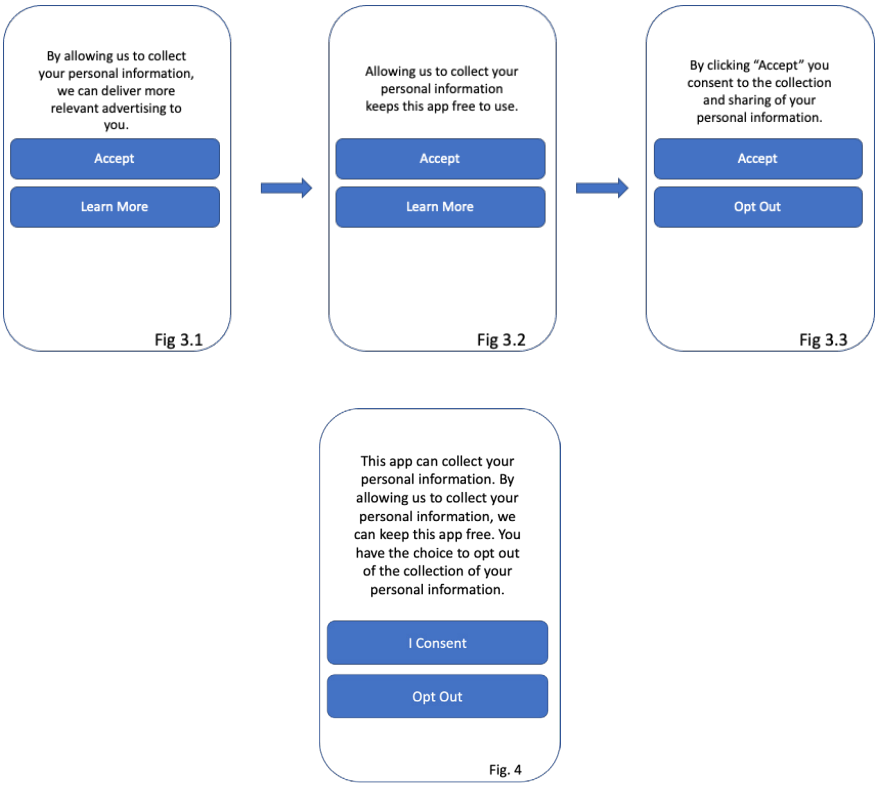
- Ensure visual presentation of information is not unduly burdensome or deceptive.

47 *See In re PaymentsMD, LLC*, F.T.C. File No.132 3088 (Jan. 27, 2015).



In Fig. 1, above, the language used and the options presented in the interstitial notice are unclear. Compare to Fig. 2, where the user is instructed what clicking "Accept" means.

- Avoid confusing sentence structure.
- Ensure the opt out link is on the same page as the accept button



In Fig. 3, above, the user must click through three pages of information before being presented with the option to opt out. Compare with Fig. 4, where the relevant information and the opt-out option are presented in a single screen.

- Ensure that any toggles or sliders clearly explain which selection results in which outcome.

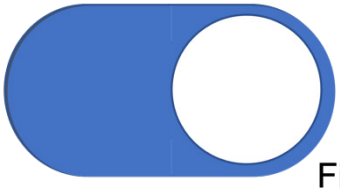


Fig. 5

Opt out of targeted advertising.

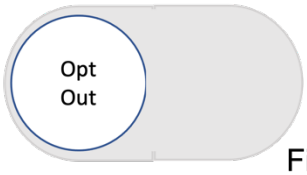


Fig. 6.1

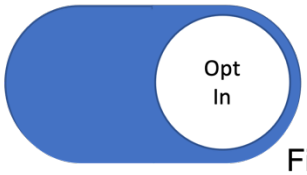


Fig. 6.2

Adjust your preferences for targeted advertising.

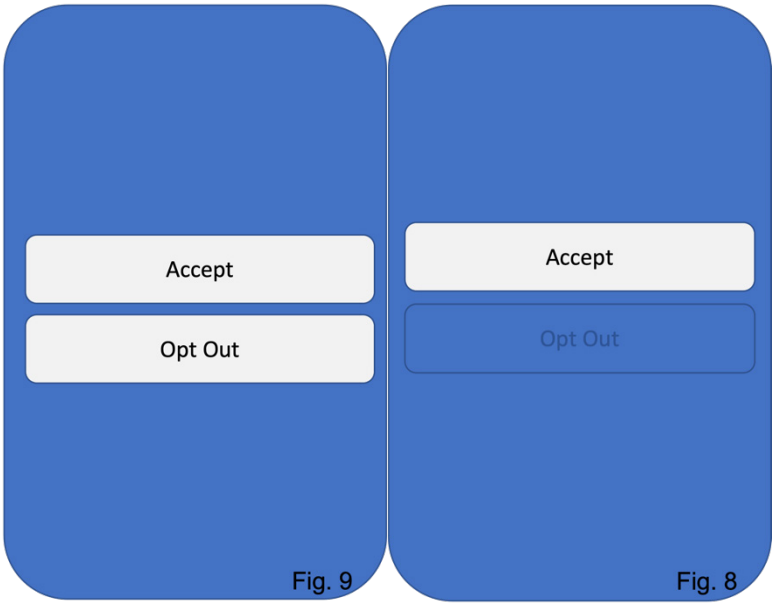
In Fig. 5, above, the toggle button's instructions do not indicate when a user has opted out of targeted advertising. Compare with Figs. 6.1 and 6.2, where the instructions are more direct, and opting out and accepting are visually distinct.

- Ensure just-in-time-notices are clear and distinct.
- Avoid inferring a user's choice or consent based on closing a pop-up window.

Fig. 7

In Fig. 7, above, the user is not presented with any meaningful choice. Instead, the UI design infers consent, and requires additional steps the user must take if she wants to opt out.

- Avoid displaying a custom message that mirrors the functionality of a system alert.
- Avoid designs or techniques that may be blocked by standard browser settings.
- Use notice/choice font sizes that are readable to a reasonable standard and consistent with other site or page content; use font colors that contrasted from the respective background of the page and/or respective action buttons.



In Fig. 8, above, the "Accept" button is in a color distinct from the background, while the "Opt Out" button is hidden with a similar color scheme. Compare with Fig. 9, where the "Accept" and "Opt Out" buttons are the same color, distinct against the background and easy to read.

- Notify consumers of the ability to change their selection and how to do so.

5. Appendix

A. Enforcement Cases

a. Disclosure omissions

FTC v. AH Media Group, LLC (2019)
Overview: FTC brought an action against AH Media Group, alleging deceptive acts or practices under the FTC Act. AH Media was fined $4.3 million for defrauding consumers.

Business Practices and Dark Patterns: AH Media offered low-cost trials of their skin care products, but after a two-week period enrolled consumers into a continuity plan without consumers' knowledge.[1] AH Media's landing pages "create[d] a sense of urgency by stating that there [was] a limited supply of the trial product and that consumers need[ed] to act quickly."[2] However, these landing pages did not include clear and conspicuous disclosures explaining the terms of the offer.[3] When there were links to the applicable terms and conditions, the links were located at the bottom of the page in a small gray font.[4]

Disposition: AH Media was ordered to pay $4.3 million by the U.S. District Court for the Northern District of California.[5]

FTC v. Office Depot, Inc. (2019)
Overview: FTC brought an action against Office Depot and its tech-support services vendor, Support.com, alleging deceptive acts or practices under the FTC Act. Office Depot settled the case for $25 million, and its vendor Support.com settled for $10 million.

Business Practices and Dark Patterns: Office Depot and its vendor, Support.com, ran a tech support service from around 2009 to 2016 as a "PC Health Check Program." The Health Check Program was advertised as a free service to consumers, although it was designed as a tool to sell diagnostic and repair services.[6] Office Depot knew that checking any box in the Health Check Program would result in an automatically suggested software repair.[7] Support.com knew as well.[8]

Disposition: Office Max settled with the FTC for $25 million, and Support.com settled with the FTC for $10 million.[9]

In re PayPal, Inc. (2018)
Overview: FTC alleged PayPal misled users about the availability of funds transferred in its peer-to-peer payment app, Venmo.

1 First Am. Compl. at 5, *Fed. Trade Comm'n v. AH Media, LLC*, No. 19-cv-04022-JD, ECF No. 74 (N.D. Cal. Oct. 23, 2019).
2 *Id.* at 7.
3 *Id.* at 8.
4 *Id.*
5 Press Release, FTC Halts Online Subscription Scheme that Deceived People with "Free Trial" Offers (May 8, 2020) (https://www.ftc.gov/news-events/press-releases/2020/05/ftc-halts-online-subscription-scheme-deceived-people-free-trial).
6 Compl. at 5, *Fed. Trade Comm'n v. Office Depot, Inc.*, No. 9:19-cv-80431, ECF No. 1 (S.D. Fla. Mar. 27, 2019).
7 *Id.* at 18.
8 *Id.* at 19.
9 Press Release, Federal Trade Commission, Office Depot and Tech Support Firm Will Pay $35 Million to Settle FTC Allegations That They Tricked Consumers into Buying Costly Computer Repair Services (Mar. 27, 2019) (https://www.ftc.gov/news-events/press-releases/2019/03/office-depot-tech-support-firm-will-pay-35-million-settle-ftc).

Business Practices and Dark Patterns: When a Venmo user sent money to another, a push notification would be sent to the recipient seconds after the sender initiated the transfer.[10] In the push notifications and on Venmo's homepage, Venmo represented that a user would get access to the money "overnight."[11] However, in many instances Venmo did not able users to access their money overnight, which resulted in "many thousands" of user complaints to Venmo.[12] Internal Venmo emails showed that the company was aware of user frustration and confusion; however, the company continued to represent that users could access money overnight.[13]

Disposition: PayPal settled with the FTC and agreed to no longer misrepresent material restrictions on accessibility of transferred money.[14]

In re PaymentsMD, LLC (2015)
Overview: FTC alleged PaymentsMD deceptively enticed consumers to consent to the collection of sensitive health information from third parties. PaymentsMD settled with the FTC, destroying the sensitive health information it collected related to the service.

Business Practices and Dark Patterns: PaymentsMD developed a service called Patient Health Report, a fee-based service that would enable consumers to access, review, and manage health records.[15] This information would be collected from health insurance plans, pharmacies, and medical testing labs.[16] The Patient Health Report registration page contained four lengthy authorizations, which could only display a few lines of text at a time.[17] Consumers could select a single check box, which would consent to all four authorizations.[18] At no point on the registration page was it clearly and conspicuously disclosed that consumers were authorizing the collection of sensitive health information.[19]

Disposition: PaymentsMD settled with the FTC and agreed to destroy the sensitive health information it had collected.[20]

b. Misrepresentation data collection, use or sharing

FTC v. NutraClick LLC (2020)
Overview: NutraClick, a dietary supplement and beauty products business, settled a case with the FTC in 2016 over charges that it offered consumers free samples of their products but then charged consumers a monthly fee without consumers' consent. In 2020, the FTC brought a second case against NutraClick, alleging it was violating its consent order. NutraClick settled with the FTC for $1.04 million.

Business Practices and Dark Patterns: NutraClick enrolled consumers in paid "VIP Membership" programs after consumers signed up for a free trial period for their dietary supplements and beau-

10 Compl. at 2, *In re PayPal, Inc.*, F.T.C. File No. 162 3102 (May 23, 2018).
11 *Id.* at 3.
12 *Id.* at 4.
13 *Id.*
14 Decision, *In re PayPal, Inc.*, F.T.C. File No. 162 3102 (May 23, 2018).
15 Compl. at 2, *In re PaymentsMD, LLC*, F.T.C. File No.132 3088 (Jan. 27, 2015).
16 *Id.*
17 *Id.* at 5.
18 *Id.*
19 *Id.* at 7.
20 Decision, *In re PayemntsMD, LLC*, F.T.C. File No. 132 3088 (Jan. 27, 2015).

ty products.[21] NutraClick failed to clearly and conspicuously disclose to consumers that they must call the company at least one day before the end of the free trial period to avoid being charged for a monthly membership program.[22] Typically, NutraClick would charge consumers the full price of the membership at 4:00 AM Eastern Time on the last day of the free trial period.[23]

Disposition: NutraClick settled with the FTC for $1.04 million, and agreed to no longer use negative option marketing.[24]

FTC v. Age of Learning, Inc. (2020)
Overview: FTC brought an action against Age of Learning, Inc. (d/b/a ABCmouse.com), alleging deceptive acts or practices under the FTC Act. Age of Learning settled for $10 million.

Business Practices and Dark Patterns: On its signup page, Age of Learning represented that membership cost either $59.95 for 12 months or four equal installments of $19.75.[25] In addition, Age of Learning also represented users could cancel their membership at any time.[26] However, Age of Learning did not disclose on its membership signup page that memberships automatically renewed every year.[27] For consumers to find the actual terms of the membership, users were required to visit separately hyperlinked terms and conditions.[28] Even then, the information disclosed was in a font smaller than the rest of the text on the page, near the bottom of a lengthy list of terms and conditions.[29] In internal documentation, Age of Learning acknowledged that consumers found the terms and conditions of their website "misleading."[30]

Disposition: Age of Learning settled with the FTC for $10 million, with more than $9.7 million going to 206,814 consumers for refunds.[31]

FTC v. AH Media Group, LLC (2019)
Overview: FTC brought an action against AH Media Group, alleging deceptive acts or practices under the FTC Act. AH Media was fined $4.3 million for defrauding consumers.

Business Practices and Dark Patterns: AH Media's payment pages stated repeatedly that the total cost of the trial product was equal only to the cost of shipping and handling.[32] AH Media's checkout pages likewise did not state there were additional costs or any additional terms and conditions to which consumers were agreeing.[33] When consumers completed the checkout, AH Media enrolled consumers in a continuity plan that cost up to $90 a month.[34]

---

21 Compl. at 4, *Fed. Trade Comm'n v. NutraClick, LLC*, No. 2:20-cv-08612, ECF No. 1 (Sept. 21, 202).
22 *Id.*
23 *Id.* at 5.
24 Press Release, NutraClick LLC to Pay $1.04 Million and Agree to Negative Option Marketing Ban to Settle FTC Allegations That It Violated 2016 Court Order (Sept. 22, 2020) (https://www.ftc.gov/news-events/press-releases/2020/09/nutraclick-to-pay-1-million-and-agree-to-marketing-ban).
25 *Id.* at 5.
26 *Id.*
27 *Id.* at 6.
28 *Id.* at 7.
29 *Id.*
30 *Id.* at 8.
31 Press Release, FTC Sends Refunds to Consumers Unfairly Billed for ABCmouse Memberships (Apr. 19, 2021) (https://www.ftc.gov/news-events/press-releases/2021/04/ftc-sends-refunds-consumers-unfairly-billed-abcmouse-memberships).
32 *Id.* at 9.
33 *Id.* at 11.
34 *Id.* at 5.

Disposition: AH Media was ordered to pay $4.3 million by the U.S. District Court for the Northern District of California.[35]

FTC v. Office Depot, Inc. (2019)
Overview: FTC brought an action against Office Depot and its tech-support services vendor, Support.com, alleging deceptive acts or practices under the FTC Act. Office Depot settled the case for $25 million, and its vendor Support.com settled for $10 million.

Business Practices and Dark Patterns: Office Depot's PC Health Check Program would ask consumers one of four questions about PC performance; no matter the answer, they would alert that their program had identified malware on their computers when, in fact, it had not done so.[36]

Disposition: Office Depot settled with the FTC for $25 million, and Support.com settled with the FTC for $10 million.[37]

c. Interfering with User Choice

i. Disparate visual options to obfuscate alternatives

In re Zoom Video Communications, Inc. (2020)
Overview: FTC brought an action against Zoom, alleging Zoom circumvented user privacy controls for consumers using the Safari browser. Zoom settled with the FTC, putting in place a new information security program with more stringent reporting and recordkeeping requirements.

Business Practices and Dark Patterns: In July 2018, Zoom updated its App for Mac computers by deploying a web server onto users' computers to circumvent a privacy and security safeguard in Safari.[38] Apple had installed a safeguard that deployed a pop up box to confirm a user wanted a page in Safari to open an app (such as Zoom). Zoom issued a manual update to its software that bypassed the Safari safeguard.[39] The end result was Zoom would automatically join a consumer to a Zoom Meeting and open their webcam without the consumer's consent—despite explicit controls in Safari that allowed consumers to request consent before an app did so.[40]

Disposition: Zoom settled with the FTC, implementing new security measures and agreeing to comply with new reporting and recordkeeping requirements.[41]

In re PayPal, Inc. (2018)
Business Practices and Dark Patterns: The FTC alleged Venmo deceptively represented consumer privacy controls in its app. Venmo's default privacy settings could be set to one of three options for visibility of account activity: Public (*i.e.*, visible to everyone); Friends (*i.e.*, only visible to friends of the sender or the recipient); or Participants Only (*i.e.*, only visible to the sender and recipient).[42]

35 Press Release, FTC Halts Online Subscription Scheme that Deceived People with "Free Trial" Offers (May 8, 2020) (https://www.ftc.gov/news-events/press-releases/2020/05/ftc-halts-online-subscription-scheme-deceived-people-free-trial).
36 *Id.* at 2.
37 Press Release, Federal Trade Commission, Office Depot and Tech Support Firm Will Pay $35 Million to Settle FTC Allegations That They Tricked Consumers into Buying Costly Computer Repair Services (Mar. 27, 2019) (https://www.ftc.gov/news-events/press-releases/2019/03/office-depot-tech-support-firm-will-pay-35-million-settle-ftc).
38 Compl. at 8, *In re Zoom Video Communications, Inc.*, F.T.C. File No. 192 3167 (Jan. 19, 2021).
39 *Id.*
40 *Id.* at 9.
41 Decision, *In re Zoom Video Communications, Inc.*, F.T.C. File No. 192 3167 (Feb. 1, 2021).
42 *Id.* at 7.

However, in order to control the visibility of transactions, a user had to go to a second page to "Transaction Sharing Settings," where by default transaction sharing was set to "Everyone."[43] This resulted in consumers who set their privacy settings to Participants Only to still have their transactions published in Venmo feeds.

Disposition: PayPal settled with the FTC and agreed to no longer misrepresent material restrictions on accessibility of transferred money and user privacy controls.[44]

In re PaymentsMD, LLC (2015)
Overview: FTC alleged PaymentsMD deceptively enticed consumers to consent to the collection of sensitive health information from third parties through its Patient Health Report program. PaymentsMD settled with the FTC, destroying the sensitive health information it collected related to the service.

Business Practices and Dark Patterns: The Patient Health Report registration page contained four lengthy authorizations, which could only display a few lines of text at a time.[45] Consumers could select a single check box, which would consent to all four authorizations.[46] At no point on the registration page was it clearly and conspicuously disclosed that consumers were authorizing the collection of sensitive health information.[47]

Disposition: PaymentsMD settled with the FTC and agreed to destroy the sensitive health information it had collected.[48]

ii. **Burdensome cancellations** (for our industry think opt outs)

CNIL: Google.fr and Facebook Ireland (2022)
Overview: The French data protection agency, CNIL, alleged Google.fr and Facebook Ireland did not provide an adequate opt out button for French users to decline to accept cookies.[49]

Business Practices and Dark Patterns: Google.fr and Facebook Ireland offered a button allowing users to immediately accept cookies on their platforms. However, there was no equivalent button allowing users to decline to accept cookies. Instead, multiple clicks were required to refuse all cookies, compared to a single one to accept all of them.

Disposition: Google.fr was fined €150 million ($170 million USD); Facebook Ireland was fined €60 million ($67.9 million USD).[50]

FTC v. Age of Learning, Inc. (2020)
Business Practices and Dark Patterns: For consumers to find the actual terms of membership on ABCmouse.com, users were required to visit separately hyperlinked terms and conditions.[51] Even

43 *Id.*
44 Decision, *In re PayPal, Inc.*, F.T.C. File No. 162 3102 (May 23, 2018).
45 *Id.* at 5.
46 *Id.*
47 *Id.* at 7.
48 Decision, *In re PayemntsMD, LLC*, F.T.C. File No. 132 3088 (Jan. 27, 2015).
49 Press Release, Cookies: the CNIL Fines Google a Total of 150 Million Euros and Facebook 60 Million Euros for Non-Compliance with French Legislation (Jan. 6, 2022) (https://www.cnil.fr/en/cookies-cnil-fines-google-total-150-million-euros-and-facebook-60-million-euros-non-compliance).
50 *Id.*
51 *Id.* at 7.

then, the information disclosed was in a font smaller than the rest of the text on the page, near the bottom of a lengthy list of terms and conditions.[52] In internal documentation, Age of Learning acknowledged that consumers found the terms and conditions of their website "misleading." When consumers actually tried to cancel their accounts with Age of Learning, the process was cumbersome. To get to the cancellation page, users had to navigate from the "My Account" section of ABCmouse.com to the "Membership" page, where a separate link took them to a "Customer Support" page. From the "Customer Support" page, users had to navigate through frequently asked questions before finding a link labeled "Contact Us" that brought up an email address.[53] However, when sending a cancellation email to that address, Age of Learning responded to consumers saying that they could not cancel their accounts via email.[54] When consumers could finally reach the cancellation page on ABCmouse.com, they had to navigate through several pages of promotions and links that, when clicked, took consumers away from the cancellation page.[55] There were a total of between six and nine screens consumers were required to navigate before they could cancel their accounts.[56]

Disposition: Age of Learning settled with the FTC for $10 million, with more than $9.7 million going to 206,814 consumers for refunds.[57]

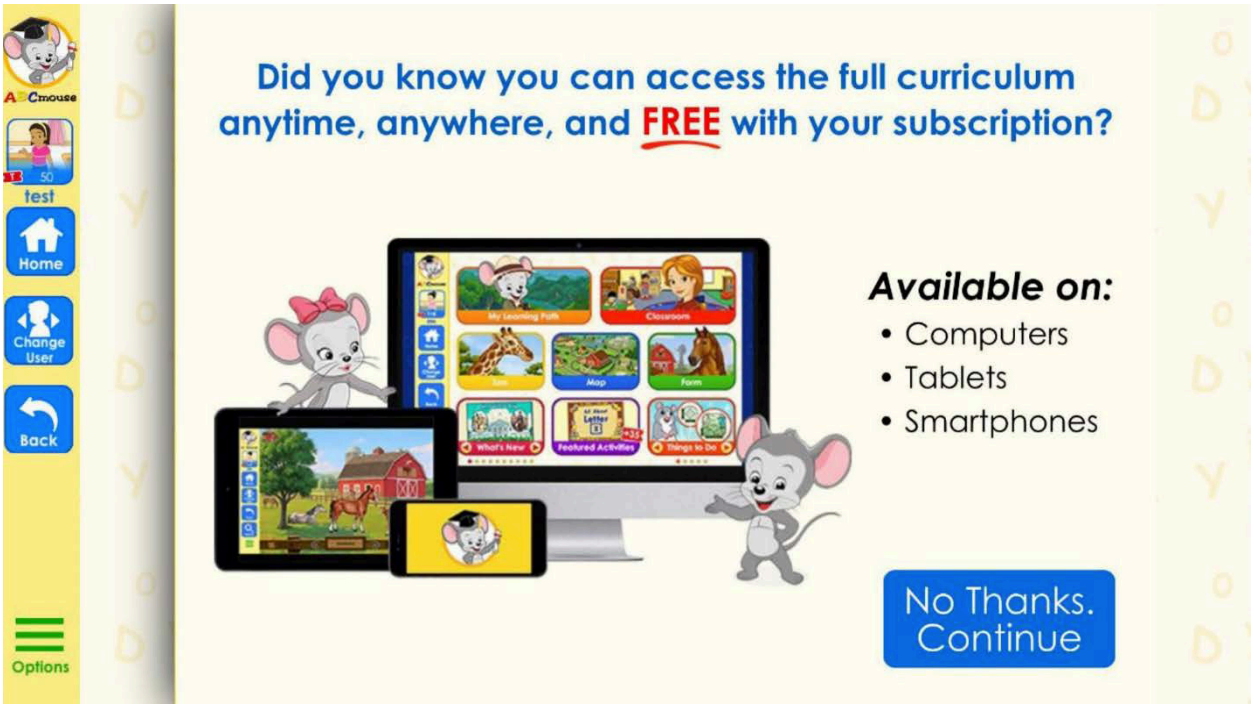
FTC v. AH Media Group, LLC (2019)
Business Practices and Dark Patterns: AH Media's payment pages stated repeatedly that the total cost of the trial product was equal only to the cost of shipping and handling.[58] AH Media's checkout pages likewise did not state there were additional costs or any additional terms and conditions to which consumers were agreeing.[59] When consumers completed the checkout, AH Media enrolled consumers in a continuity plan that cost up to $90 a month.[60]

Disposition: AH Media was ordered to pay $4.3 million by the U.S. District Court for the Northern District of California.[61]

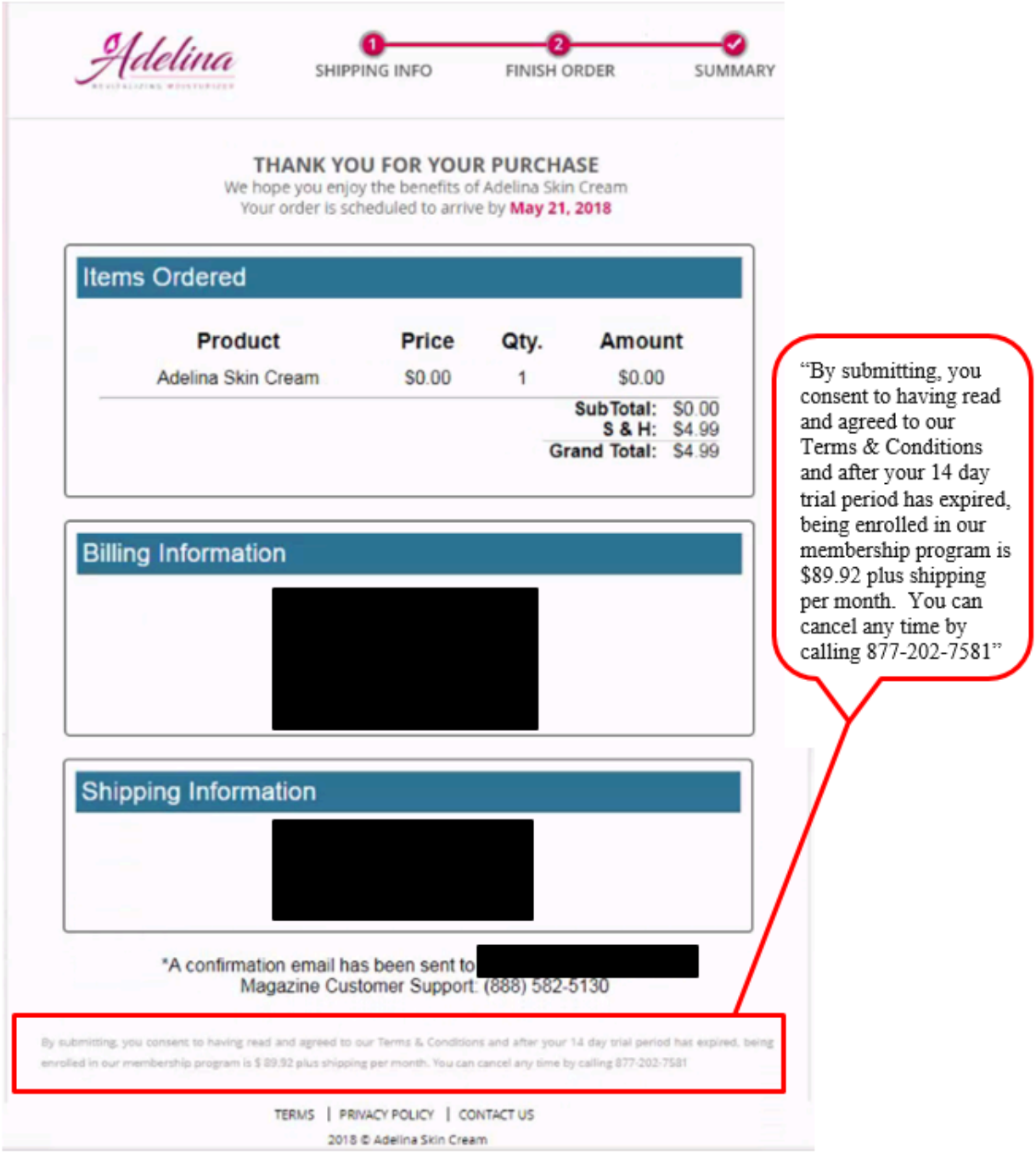
B. Examples of Dark Patterns from FTC Cases

These visual examples come directly from cases brought by the FTC.

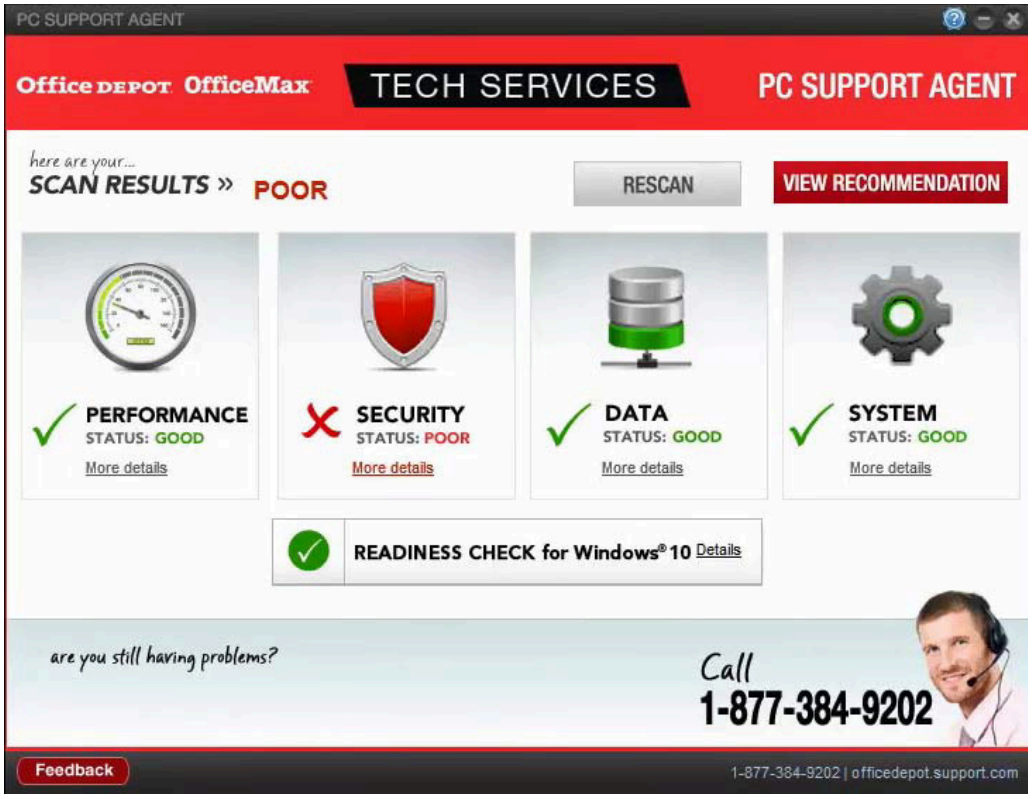
52 *Id.*
53 *Id.* at 10-11.
54 *Id.* at 10.
55 *Id.* at 11.
56 *Id.* at 15.
57 Press Release, FTC Sends Refunds to Consumers Unfairly Billed for ABCmouse Memberships (Apr. 19, 2021) (https://www.ftc.gov/news-events/press-releases/2021/04/ftc-sends-refunds-consumers-unfairly-billed-abcmouse-memberships).
58 First Am. Compl. at 9, *Fed. Trade Comm'n v. AH Media, LLC*, No. 19-cv-04022-JD, ECF No. 74 (N.D. Cal. Oct. 23, 2019).
59 *Id.* at 11.
60 *Id.* at 5.
61 Press Release, FTC Halts Online Subscription Scheme that Deceived People with "Free Trial" Offers (May 8, 2020) (https://www.ftc.gov/news-events/press-releases/2020/05/ftc-halts-online-subscription-scheme-deceived-people-free-trial).

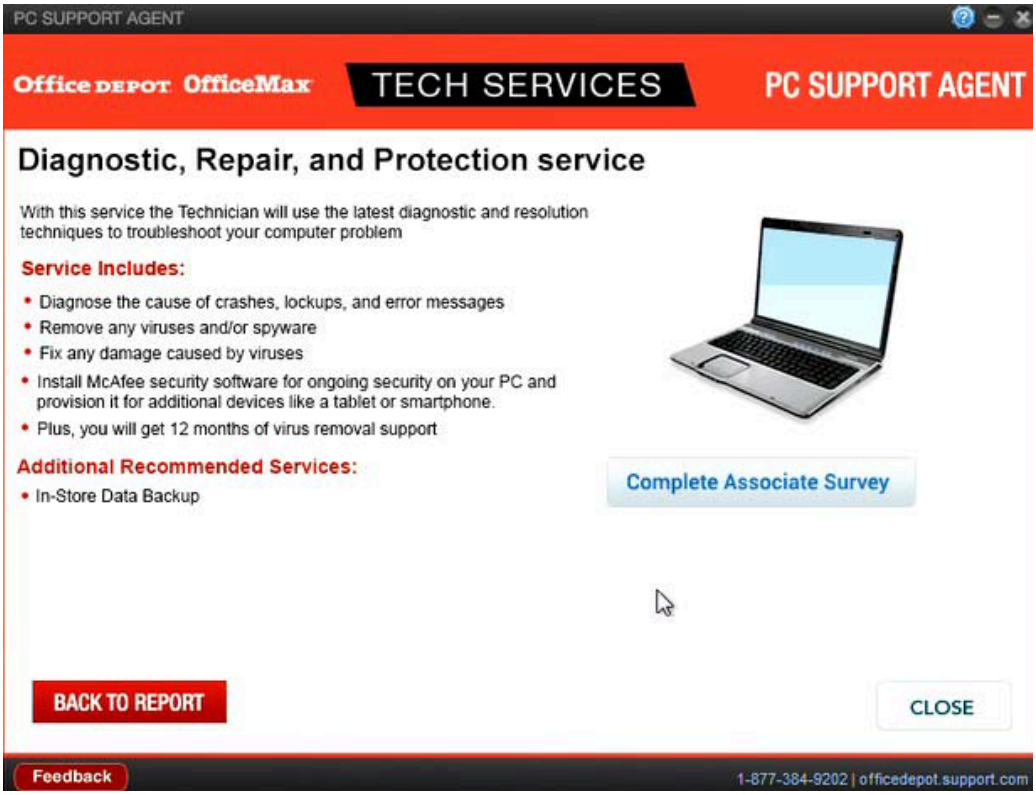


Burdensome Cancellation: ABCmouse.com required users to go through a lengthy path to cancel accounts, beginning with this page. Nowhere on the page does the word "Cancellation" appear. (From *FTC v. Age of Learning, Inc.*, No. 2:20-cv-7996, ECF No. 1 (C.D. Call. Sept. 1, 2020).)



Disparate Visual Options: The full terms of AH Media's service were presented in a small, gray font against a white background. (From *FTC v. AH Media, LLC*, No. 19-cv-04022-JD, ECF No. 74 (N.D. Cal. Oct. 23, 2019).)





Omissions: The PC Health Check Program would always state that scan results found malware on the user's PC, urging the purchase of Office Max's security services. (From *FTC v. Office Depot, Inc.*, No. 9:19-cv-80431, ECF No. 1 (S.D. Fla. Mar. 27, 2019).)