



May 28, 2021

## Comments of the Computer & Communications Industry Association Regarding the FTC Workshop on “Bringing Dark Patterns to Light” (FTC-2021-0019)

Pursuant to the request for comments issued by the Federal Trade Commission (FTC or the Commission) regarding topics discussed at the Dark Patterns Workshop (the Workshop) held on April 29, 2021,<sup>1</sup> the Computer & Communications Industry Association (CCIA) submits the following comments.

CCIA is an international, not-for-profit trade association representing a broad cross section of communications and technology firms. For nearly fifty years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than \$100 billion in research and development, and contribute trillions of dollars in productivity to the global economy.<sup>2</sup>

CCIA thanks the Commission for its attention to this topic and consideration of these comments. The Workshop provided diverse expert perspectives that drew attention to deceptive and manipulative design practices in website and mobile technology interfaces as well as substantive discussion of approaches to preventing consumer harm that can result from such designs. CCIA submits these comments to emphasize, respond, and provide additional context to certain points raised by Workshop participants.

### I. A Note on Terminology

Rather than employ the terminology of “dark patterns,” these comments will refer to “manipulative design” practices or interfaces unless directly quoting the Workshop or another source. We believe this is more precise and appropriate terminology for referring to the unlawful and harmful practices examined at the Workshop for several reasons. First, many of the design characteristics discussed as “dark patterns” during the Workshop are not limited to digital interfaces but are longstanding unfair and deceptive practices that have been subject to enforcement in offline contexts.<sup>3</sup> Second, as indicated during the Workshop by Professor Harry Brignull, while the term “dark pattern” (originated and popularized in part by Brignull) has been useful for marketing and raising awareness, it would be both “vague and sloppy” if used as a legal term or standard.<sup>4</sup> Increased definitional precision will be highly desirable if policymakers or regulators seek to develop guidance concerning manipulative design practices. Given the apparent academic consensus that the boundaries of “dark pattern” designs are inherently indefinite, (a “Wittgensteinian family of concepts” as described by one

---

<sup>1</sup> Federal Trade Commission, “Request for Comments Regarding Topics to be Discussed at Dark Patterns Workshop” (Apr. 9, 2021), <https://www.regulations.gov/document/FTC-2021-0019-0001>.

<sup>2</sup> A list of CCIA members is available at <https://www.cciagnet.org/members>.

<sup>3</sup> See Evan Rose, FTC Dark Patterns Workshop Transcript (“Workshop Transcript”) at 66 (Apr. 29, 2021), *available at* [https://www.ftc.gov/system/files/documents/public\\_events/1586943/ftc\\_darkpatterns\\_workshop\\_transcript.pdf](https://www.ftc.gov/system/files/documents/public_events/1586943/ftc_darkpatterns_workshop_transcript.pdf) (“We also know that many of these design techniques are not new. Many have long existed in the brick and mortar context.”).

<sup>4</sup> See Harry Brignull, Workshop Transcript at 14-15.

Workshop participant),<sup>5</sup> relying upon such terminology is unlikely to deliver clear and actionable guidance for user-interface and product designers or compliance counsel. Finally, we note that there is broad consensus and efforts underway in the technology community to promote inclusivity by replacing computer engineering terms that are rooted in the connection of “dark-light dualism” to judgments about morality, which is a characteristic of “dark patterns” terminology.<sup>6</sup>

## II. The Commission Is Well Equipped to Enforce Against Unlawful Manipulative Design Practices Under Its Existing Authority

The Commission has clear authority to enforce against manipulative design by virtue of its tools to combat “unfair or deceptive acts or practices” pursuant to Section 5 of the Federal Trade Commission Act.<sup>7</sup> Consistent with both statute and precedent, to the extent that a design practice entails a misleading representation or omission that is material, it is actionable under the “deception” prong of the Commission’s authority.<sup>8</sup> Similarly, to the extent that a design practice is likely to result in consumer injury that is neither reasonably avoidable nor outweighed other market benefits, it is actionable under the “unfairness” prong of the Commission’s authority.<sup>9</sup>

The FTC’s firm statutory grounds to enforce against such manipulative design practices in digital contexts was directly addressed by Commissioner Chopra in a statement connected to *Age of Learning, Inc.*, recognizing that “[d]igital deception should not be a viable American business model.”<sup>10</sup> Commissioner Chopra further noted that the Commission “has numerous tools to root out the kinds of tricks and traps we saw in this matter,” citing the Restore Online Shoppers’ Confidence Act, the CAN-SPAM Act, and, significantly, the FTC Act itself.<sup>11</sup> Indeed, the Commission has an extensive history of successful enforcement actions for both restitution and injunctive relief involving many of the manipulative design practices and interfaces that have been described as “dark patterns” in recent years. Below is a partial list of relevant enforcement actions against specific examples of manipulative design practices that were discussed at the Workshop.

### Manipulative designs that steer users towards taking a particular action:<sup>12</sup>

- *In re PaymentsMD, LLC* (2015): This complaint involved the patient registration process for an online provider of billing services to medical providers. The Commission alleged that the Respondent’s online registration process misled consumers into allowing the Respondent to

---

<sup>5</sup> Workshop Presentation of Arunesh Mathur describing different themes of “dark patterns”, Panel 1.

<sup>6</sup> See, e.g., Kat Zhou, Workshop Transcript at 15; Kate Conger, “‘Master,’ ‘Slave’ and the Fight Over Offensive Terms in Computing,” *The New York Times* (Apr. 13, 2021), <https://www.nytimes.com/2021/04/13/technology/racist-computer-engineering-terms-ietf.html>.

<sup>7</sup> 15 U.S.C. § 45(a)(1). See also Jamie Luguri & Lior J. Strahilevitz, “Shining a Light on Dark Patterns,” 13 *Journal of Legal Analysis* 43, 90 (2021), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3431205](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205) (“[T]his survey of the existing precedents suggests that the law restricting dark patterns does not need to be invented; to a substantial degree it is already present.”).

<sup>8</sup> FTC Policy Statement on Deception (Oct. 14, 1983), [https://www.ftc.gov/system/files/documents/public\\_statements/410531/831014deceptionstmt.pdf](https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf).

<sup>9</sup> U.S.C. § 45(n).

<sup>10</sup> Commissioner Rohit Chopra, “Regarding Dark Patterns in the Matter of *Age of Learning, Inc.*” Federal Trade Commission (Sept. 2, 2020), [https://www.ftc.gov/system/files/documents/public\\_statements/1579927/172\\_3086\\_abcmouse\\_-\\_rchopra\\_statement.pdf](https://www.ftc.gov/system/files/documents/public_statements/1579927/172_3086_abcmouse_-_rchopra_statement.pdf).

<sup>11</sup> *Id.*

<sup>12</sup> See Senator Mark Warner, Workshop Transcript at 3: “Consumers, basically, looking for information or looking for an answer, are basically greeted with screenshot after screenshot, where virtually the only option is to agree. You have to go through a series of hoops and hurdles to ever kind of get out of that page, to say no, to say, I don’t want to opt in and opt out.”

collect personal health information from third parties. In the Commission’s view, “the site design simultaneously made it hard to read the authorizations in their entirety, and easy to skip over them by clicking a single check box that preceded all of the authorizations.” The Commission further argued that at “no point in registering for the Patient Portal would it have been clear to the consumer that they were purportedly giving respondent permission to obtain their sensitive health information from third parties. . . .”<sup>13</sup>

- *FTC v. Office Depot, Inc. & Support.com, Inc.* (2019): This case involved the sale of computer diagnostic and repair services connected to the results of running a free virus scanning service on customers’ computers. The Commission alleged that Defendants “bilked unsuspecting consumers out of tens of millions of dollars from their use of the PC Health Check Program to sell costly diagnostic and repair services.” The complaint specifically alleged that while Defendants represented that the software program was finding infections or malware symptoms on customer computers, it was “designed as a sales tool” and presented results that were based entirely on how consumers answered a questionnaire that they received at the beginning of the program.<sup>14</sup>
- *FTC v. AH Media Group, LLC, et al.* (2019): This case involved online advertisements and registration for subscription-based membership plans for purchasing beauty products. The Commission alleged that the Defendants’ consumer-facing websites buried material information about enrollment in continuity plans “in small terms and conditions links, and in statements displayed in small font size and light-colored text that appear only after a consumer orders a product.”<sup>15</sup> The resulting stipulated order barred the Defendants from engaging in marketing that made use of “Negative Option Feature[s]” in which the absence of an affirmative action is interpreted as consent to be charged for goods or services.<sup>16</sup>

Manipulative designs that mislead consumers into registering for “free” trials that are difficult if not impossible to cancel:<sup>17</sup>

- *FTC v. Bunzai Media Group, Inc. et al.* (2015): This case involved online advertisements (including pop-up banners) and websites offering “risk-free” trials for skincare products. The Commission alleged that Defendants’ websites did not display disclosures concerning “initial charges for the product, continuity program, or return policies until the ‘final step’ of the Defendants’ ordering page” and that the disclosure “is in significantly smaller print and is obscured by a variety of graphics and text”. The Commission further alleged that Defendants’ websites “use deceptive pop-up advertisements that discourage consumers from leaving Defendants’ websites without

---

<sup>13</sup> *In the Matter of PaymentsMD, LLC*, Docket No. C-4505 (Jan. 27, 2015),

<https://www.ftc.gov/system/files/documents/cases/150206paymentsmdcmpt.pdf>.

<sup>14</sup> *FTC v. Office Depot, Inc., & Support.com, Inc.*, Case No. 9:19-cv-804321, S.D. Fla. (Mar. 27, 2019),

[https://www.ftc.gov/system/files/documents/cases/office\\_depot\\_complaint\\_3-27-19.pdf](https://www.ftc.gov/system/files/documents/cases/office_depot_complaint_3-27-19.pdf).

<sup>15</sup> *FTC v. AH Media Group, LLC et al.*, Case No. 3:19-cv-04022-JD, N.D. Cal. (July 12, 2019),

[https://www.ftc.gov/system/files/documents/cases/ah\\_media\\_complaint.pdf](https://www.ftc.gov/system/files/documents/cases/ah_media_complaint.pdf).

<sup>16</sup> Stipulated Order for Permanent Injunction and Monetary Judgment, *FTC v. AH Media Group, LLC*, Case No. 3:19-cv-04022-JD, N.D. Cal. (Mar. 6, 2020), <https://www.ftc.gov/system/files/documents/cases/ahmediaorderschillzanelo.pdf>.

<sup>17</sup> See Workshop Comments of Representative Lisa Blunt Rochester at 4: “Now, free trials are a common enough experience that we’ve all had. But the real issue, as I continue to read into the reviews, was that canceling your trial wasn’t nearly as easy as signing up for it. There was no obvious button to cancel the trial, no prominent link to navigate to. And the users were left guessing if deleting the app altogether would cancel the subscription as well.”

accepting a trial offer” including false assertions of Better Business Bureau accreditation and ratings.<sup>18</sup>

- *FTC v. Triangle Media Corp. et al.* (2018): This case involved online advertisements (including through blog posts, banner advertisements, and surveys) and websites that offered “RISK FREE” trials for skincare products, e-cigarettes, and dietary supplements. The Commission alleged that Defendants sent consumers deceptive order confirmation emails that did not list unexpected additional charges and that Defendants made it difficult for consumers to cancel their subscriptions due to restrictive cancellation policies and limited availability of customer service representatives, even for customers who called numerous times. The Commission further alleged that the Defendants’ websites “create a sense of urgency by telling consumers there is a limited supply of the trial product and that they need to act quickly.”<sup>19</sup>
- *FTC v. Age of Learning, Inc.* (2020): This case involved advertisements and the subscription process for an online childrens’ education program. The Commission alleged that despite offering “Easy Cancellation” in bold, red text, the Defendant “restricted the ways consumers could cancel their memberships, permitting cancellation only through an online mechanism within Defendant’s website and app that was difficult for consumers to find and complete. Consumers who requested cancellation via this mechanism often have believed they canceled, but Defendant continued to charge them anyway.” The complaint further alleged that the defendant failed to disclose material information about membership plans, “including that they automatically renew, that Defendant would charge members each year unless they cancel, and what consumers must do to cancel.”<sup>20</sup>

Manipulative designs or representations regarding privacy controls and software updates that may cause users to agree to or participate in disclosing personal data:<sup>21</sup>

- *In re Paypal, Inc.* (2018): This complaint involved the privacy controls of a peer-to-peer payment service. The Commission alleged that the Respondent created a set of difficult to parse privacy settings that failed to adequately disclose the public visibility of particular financial transactions. Specifically the Commission alleged that the service’s design configuration “has the effect of overriding . . . clearly expressed privacy preferences.”<sup>22</sup>
- *In re Zoom Video Communications, Inc.* (2020): This complaint involved software updates for a videoconferencing platform provider. The Commission alleged that the Respondent’s description of a software update provided to users claimed the update would fix minor bugs, failing to disclose that the update would also “install a local hosted web server” that would circumvent browser privacy and security safeguards and “remain on users’ computers even after they had deleted the App.” The Commission further alleged that the Respondent did not

---

<sup>18</sup> *FTC v. Bunzai Media Group, Inc. et al.*, Case No. 2:15-cv-04527-GW-PLA, C.D. Cal. (June 16, 2015), <https://www.ftc.gov/system/files/documents/cases/160625auravie-cmpt.pdf>.

<sup>19</sup> *FTC v. Triangle Media Corp. et al.*, Case No. 18-cv-1388-BEN-NLS, S.D. Cal. (June 22, 2018), [https://www.ftc.gov/system/files/documents/cases/triangle\\_media\\_complaint\\_for\\_perm\\_injunctn\\_bcp\\_litigation.pdf](https://www.ftc.gov/system/files/documents/cases/triangle_media_complaint_for_perm_injunctn_bcp_litigation.pdf).

<sup>20</sup> *FTC v. Age of Learning, Inc. d/b/a ABCmouse.com*, Case No. 2:20-cv-7996, C.D. Cal. (Sept. 1, 2020), <https://www.ftc.gov/system/files/documents/cases/1723086abcmousecomplaint.pdf>.

<sup>21</sup> See Acting Chairwoman Rebecca Kelly Slaughter, Workshop Transcript at 1: “[W]e increasingly see companies using dark patterns to manipulate people into giving up their personal data. . . .”

<sup>22</sup> *In re Paypal Inc.*, Docket No. C-4651 (May 23, 2018), [https://www.ftc.gov/system/files/documents/cases/1623102\\_c-4651\\_paypal\\_venmo\\_complaint\\_final.pdf](https://www.ftc.gov/system/files/documents/cases/1623102_c-4651_paypal_venmo_complaint_final.pdf).

take steps to address risks that malicious actors could exploit the local web server and that by circumventing security safeguards, “one wrong click could expose consumers to remote video surveillance by strangers through their computers’ webcams.”<sup>23</sup>

- *In re Tapjoy, Inc.* (2021): This complaint involved a mobile advertising company that offered in-app rewards to engage with advertiser content such as watching a video or taking a survey. The Commission alleged that the Respondent’s offers often required consumers to incur charges or divulge personal information but that many consumers failed to receive promised rewards upon completing an interaction. The complaint further alleged that the Respondent discouraged customer service inquiries by implementing a policy prohibiting users from submitting complaints within 24 hours of interacting with advertising partners.<sup>24</sup>

Misleading consumers by presenting advertising and marketing materials as non-commercial content:

25

- *In re Practice Fusion, Inc.* (2016): This complaint involved reviews on an online directory of healthcare providers created by a cloud-based electronic health records company. The Commission alleged that the Respondent populated the directory with reviews by soliciting feedback from healthcare providers’ patients under the guise of “help[ing] improve your service in the future.” The complaint further alleged that the Respondent represented itself as the patients’ healthcare providers in these messages, redirected patients to a survey that included a pre-checked box that falsely suggested that the reviews would be anonymous, and published survey responses that included sensitive personal health information combined with identifying information.<sup>26</sup>
- *FTC v. Match Group, Inc.* (2019): This case involves an online dating service’s advertisements to nonsubscribers. The Commission alleges that the Defendant “sent consumers misleading advertisements that tout communications from persons Defendant identified as potentially fraudulent users of Match.com and led consumers to believe that the communications are from persons interested in establishing a dating relationship with them” in order to persuade non-paying subscribers to upgrade their subscriptions.<sup>27</sup> The outcome of this matter remains pending.

---

<sup>23</sup> *In re Zoom Video Communications, Inc.*, File No. 192-3167 (Nov. 9, 2020), <https://www.ftc.gov/system/files/documents/cases/1923167zoomcomplaint.pdf>.

<sup>24</sup> *In re Tapjoy Inc.*, Docket No. C-4740 (Mar. 9, 2021), [https://www.ftc.gov/system/files/documents/cases/tapjoy\\_complaint\\_final\\_signed.pdf](https://www.ftc.gov/system/files/documents/cases/tapjoy_complaint_final_signed.pdf).

<sup>25</sup> See Lior J. Strahilevitz, Workshop Transcript at 67-68: “I think another really helpful precedent is from the Second Circuit that’s LeadClick Media. And LeadClick Media involved an entity that was selling colon cleanses and weight loss products. And their site was populated both with false testimonials for consumers that had been concocted by the company and with content that was designed to look like independent journalism, designed to look like newspaper, online newspaper articles, extolling the virtues of the product at issue, when in fact, this was fake news. It was advertising content disguised to look like news. And the Second Circuit had very little difficulty in finding that these kinds of false testimonials or misleading content constituted violations of Section 5, that this content was deceptive within the meaning of the FTC Act.” See also Federal Trade Commission, “Enforcement Policy Statement on Deceptively Formatted Advertisements” (Dec. 22, 2015), [https://www.ftc.gov/system/files/documents/public\\_statements/896923/151222deceptiveenforcement.pdf](https://www.ftc.gov/system/files/documents/public_statements/896923/151222deceptiveenforcement.pdf).

<sup>26</sup> *In re Practice Fusion, Inc.*, Docket No. C-4591 (June 8, 2016), <https://www.ftc.gov/system/files/documents/cases/160608practicefusioncmpt.pdf>.

<sup>27</sup> *FTC v. Match Group, Inc.*, Case No. 3:19-cv-02281, N.D. Tex. (Sept. 25, 2019), [https://www.ftc.gov/system/files/documents/cases/match\\_-\\_complaint.pdf](https://www.ftc.gov/system/files/documents/cases/match_-_complaint.pdf).

- *In re Sunday Riley Modern Skincare, LLC* (2019): This complaint involved reviews of cosmetics products on a major retailer’s website. The Commission alleged that the Defendant instructed employees to create multiple accounts on a retailer website using a Virtual Private Network (VPN) to leave positive reviews of the Defendant’s cosmetic products that would appear to reflect “independent experiences or opinions of impartial ordinary users of the products.”<sup>28</sup>

This survey of enforcement actions demonstrates the Commission’s ample authority to enforce against manipulative design practices. Therefore, post-Workshop consideration of enforcement against manipulative design practices should focus on how to prioritize enforcement and whether additional resources and technical capacity may be necessary for the Commission to continue carrying out its consumer protection mission in the context of manipulative design.

### III. Benign and Beneficial Practices That Do Not Constitute Manipulative Design

Participants in the Workshop identified many design practices that are clearly deceptive, unfair, and pose a significant risk of harm to consumers. However, certain design practices including user control prompts and content recommendations noted by participants are frequently used to enhance and provide value to consumers in a manner consistent with user desires and expectations. Therefore, it would be inappropriate to categorically consider these features as examples of manipulative design practices subject to Commission enforcement.

#### A. User Control and Authorization Prompts

A Workshop participant suggested that “repeated requests” such as authorization for location access or updates would constitute a “dark pattern” by way of “nagging.”<sup>29</sup> However, such user control or authorization prompts are fundamentally different from the examples of manipulative design practices featured elsewhere during the Workshop. Indeed, the Commission has rightly recognized a fundamental distinction between “dark patterns” and persuasive technologies and techniques such as “nudges.”<sup>30</sup> It is necessary to distinguish between unlawful manipulative designs and requests or prompts connected with valid business purposes that are consistent with and support both user and societal expectations and policy interests.

CCIA notes the following features of user control and authorization prompts that distinguish them from manipulative designs. First, while it is true that some prompts and requests may be perceived as unwieldy or as adding unnecessary friction to the use of a service, many of the most cumbersome of such mechanisms are the result of government mandates, such as cookie consent banners on web pages.<sup>31</sup> Second, it is often

<sup>28</sup> *In re Sunday Riley Modern Skincare, LLC*, File No. 192-3008 (Oct. 21, 2019), [https://www.ftc.gov/system/files/documents/cases/192\\_3008\\_sunday\\_riley\\_complaint\\_0.pdf](https://www.ftc.gov/system/files/documents/cases/192_3008_sunday_riley_complaint_0.pdf).

<sup>29</sup> Lior J. Strahilevitz, Workshop Transcript at 78.

<sup>30</sup> Lesley Fair, “Asking for your insights into digital dark patterns,” Federal Trade Commission (Apr. 9, 2021), <https://www.ftc.gov/news-events/blogs/business-blog/2021/04/asking-your-insights-digital-dark-patterns>.

<sup>31</sup> See Bojana Bellamy et al., “GDPR One Year In: Practitioners Take Stock of the Benefits and Challenges,” Centre for Information Policy Leadership (May 31, 2019) at 8, [https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl\\_report\\_on\\_gdpr\\_one\\_year\\_in\\_-\\_practitioners\\_take\\_stock\\_of\\_the\\_benefits\\_and\\_challenges.pdf](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_report_on_gdpr_one_year_in_-_practitioners_take_stock_of_the_benefits_and_challenges.pdf); Kate Fazzini, “Europe’s sweeping privacy rule was supposed to change the internet, but so far it’s

necessary to collect and process certain user data in order to securely and effectively provide a desired digital service or feature. For example, providing a mapping service or live directions requires use of the location information of a user. Therefore, prompts that seek opt-in consent to certain data collection and processing may be triggered by a user requesting or attempting to use a desired service and are a necessary feature of providing notice of data practices and obtaining meaningful consent.

Furthermore, as a matter of policy, website and app-developers should be encouraged and have the flexibility to develop mechanisms beyond traditional privacy notices and terms-of-service that affirmatively provide relevant and actionable disclosures and controls to consumers, such as “just-in-time notices” and “in-context” notifications.<sup>32</sup> Some online services are further experimenting with displaying periodic prompts that encourage users to review account log-ins, profile connections and visibility, settings, or to take advantage of new privacy controls.<sup>33</sup> Such notices can support consumer trust by better informing and empowering consumers to use a service consistent with their desired preferences. Finally, many software updates are socially beneficial, containing patches to critical security vulnerabilities that may have just been discovered, and update prompts can serve valuable individual and public interests.

## **B. Auto-Play Features and Content Recommendations**

Scrutiny of certain design features such as automatically playing videos or content recommendations have included suggestions that such features may constitute a form of manipulative design.<sup>34</sup> However, content recommendation features are often sought out by users that wish to discover similar content to a genre they already enjoy or who may simply wish to save time and energy looking for certain content. Therefore, these design features frequently provide clear value to users and do not feature the characteristics of deception, manipulation, or unfairness typical to the examples of harmful design raised during the Workshop or appearing in the Commission’s prior enforcement actions.

## **IV. Future Regulatory or Enforcement Efforts Should Focus on the Most Harmful and Redressable Types of Manipulative Design**

As demonstrated through the Workshop panels and comment docket, it is reasonable to expect that debate at the margins of what does and does not constitute a manipulative design practice to continue. While future guidance may help to resolve some of these difficult line-drawing issues,<sup>35</sup> CCIA recommends that any subsequent regulatory or enforcement agenda continue to prioritize actions against manipulative design practices that cause clear harm. Examples of such practices include features that restrict or prevent individuals from canceling ongoing subscription services or deceptive practices that add unwanted items or

---

mostly created frustration for users, companies, and regulators,” CNBC (May 5, 2019), <https://www.cnbc.com/2019/05/04/gdpr-has-frustrated-users-and-regulators.html>.

<sup>32</sup> See, e.g., Florian Schaub et al., “A Design Space for Effective Privacy Notices,” Proc. 11th Symp. Usable Security and Privacy (2015), available at [https://www.ftc.gov/system/files/documents/public\\_comments/2015/10/00038-97832.pdf](https://www.ftc.gov/system/files/documents/public_comments/2015/10/00038-97832.pdf).

<sup>33</sup> See, e.g., Coral Murphy Marcos, “Snapchat to launch feature that prompts users to review their friends lists,” USA Today (Feb. 9, 2021), <https://www.usatoday.com/story/tech/2021/02/09/snapchats-new-feature-ask-users-review-their-friend-lists/4447403001/>; Kelly Robinson, “How to incentivize users to enable 2FA,” TwilioBlog (May 26, 2020), <https://www.twilio.com/blog/incentivize-2fa>.

<sup>34</sup> See, e.g., Josh Nelson, Workshop Transcript at 57.

<sup>35</sup> See, e.g., Ryan Calo, Workshop Transcript at 42.

charges to a purchase.<sup>36</sup> Such manipulative designs are often both the most egregious and the most redressable due to the readily calculable nature of the financial harm suffered by consumers.

## V. Pursue Definitions and Standards That Focus on Substantial Impacts, Not Intent

While degrees of complexity and ambiguity are likely to persist in efforts to define and categorize manipulative design practices, certain lessons can be drawn from the Workshop that can assist in developing practicable definitions and standards. We encourage the Commission to avoid developing definitions of manipulative design practices that rely on a determination of the “intent” of product designers and companies. Such standards would pose evidentiary and burden of proof difficulties for regulators, as well as difficulties in business compliance regimes. Furthermore, as Workshop participants noted, “intent” standards for various manipulative designs could become less relevant as new technologies and design tools emerge.<sup>37</sup> A better path forward would be to rely on “effect” or “impact” standards that can be measured objectively and are more manageable from a business compliance viewpoint.

## VI. Risks to Overly Prescriptive Regulatory Involvement in Design Practices

User-interface design is an inherently complex field that frequently involves detailed consideration, often down to the individual pixel, of how different image displays, notice terminology, process flows, and dimensions, contrasts, and colors will be perceived and engaged with by diverse user groups. Given this landscape, there would be significant likely policy and legal roadblocks to pursuing an overly prescriptive approach to regulating design features, especially across fast developing and diversifying technology platforms and devices.

The difficulty with tasking regulators to make industry-wide design choices was evident in the California Attorney General’s efforts under the California Consumer Privacy Act (CCPA). Directed to develop a “recognizable and uniform opt-out logo or button,” the California AG’s Office struggled.<sup>38</sup> The process for developing this single user control took well over a year, with the initial version of the button withdrawn following widespread criticism. Researchers observed that the button design could be interpreted as a functional toggle switch, rather than a hyperlink to a separate control page.<sup>39</sup> Worse still, the button design was shown to be reasonably interpreted by consumers as indicating that a CCPA opt-out had already taken place.<sup>40</sup>

In the fast changing technology landscape, companies are in the best position to rapidly adapt to the latest changes and best practices in design interfaces. Furthermore, appropriate consumer-directed controls and communications may vary in the context of a particular service, and those that work well for a particular browser or mobile app may not be well-suited for use with emerging technologies such as connected devices or augmented and virtual reality. Prescriptive regulation of design features may also negatively impact

---

<sup>36</sup> See FTC enforcement actions, *supra* Section II.

<sup>37</sup> See, e.g., Katharina Kopp, Workshop Transcript at 20.

<sup>38</sup> California Consumer Privacy Act, § 1798.185(a)(4)(C).

<sup>39</sup> Lorrie Faith Cranor et al., “User Testing of the Proposed CCPA Do-Not-Sell Icon” (Feb. 24, 2020), *available at*: <https://cups.cs.cmu.edu/pubs/CCPA2020Feb24.pdf>.

<sup>40</sup> *Id.*

competition on product and service features if user interface features are required to appear and function in an identical manner. Finally, strict regulation of the design of user interfaces could limit the ability of organizations to transmit complete and accurate information to users during notice and consent flows, constituting a potential infringement on businesses' First Amendment right to commercial speech.<sup>41</sup>

Given these considerations, CCIA welcomes the continuation of multistakeholder efforts on the development of best practices in user interface design as well as consumer and business education on manipulative design practices. We further recommend that the Commission maintain its focus on bringing enforcement actions to redress particular harmful practices, such as “negative option marketing,” rather than pursue the development of specific design requirements.

Thank you again for the opportunity to provide comments on this matter.

Respectfully submitted,

Keir Lamont  
Policy Counsel  
Computer & Communications Industry Association

---

<sup>41</sup> See, e.g., Justin (Gus) Hurwitz, “Designing a Pattern, Darkly,” 22:1 North Carolina Journal of Law & Technology 57, 97-100 (Oct. 2020), [https://ncjolt.org/wp-content/uploads/sites/4/2020/10/Vol.-22-Issue-1\\_Hurwitz\\_Final\\_57-106.pdf](https://ncjolt.org/wp-content/uploads/sites/4/2020/10/Vol.-22-Issue-1_Hurwitz_Final_57-106.pdf).