SIIA Comments On
"Bringing Dark Patterns to Light: An FTC Workshop"

The Software & Information Industry Association (SIIA)[1] thanks you for the opportunity to provide written comments following the FTC's April 29th workshop: *Bringing Dark Patterns to Light.* Prior to the workshop, we submitted preliminary comments that focused on topics for consideration at the workshop. We appreciated that several aspects of our comments were addressed during the workshop, including the session showcasing the work of Lior Strahilevitz and some discussion on the constitutionality of regulating dark patterns.

Our comments herein reflect upon testimony given during the workshop. We are available if our comments raise any questions or concerns. SIIA's primary contact going forward will be Christopher Mohr, General Counsel and VP Intellectual Property, who is available at cmohr@siia.net.

New Regulatory Authority is Unnecessary and Risks Unconstitutionality

As we noted in our preliminary comments ahead of the workshop, we are concerned about the growing policy agenda that is treating harmful design issues as an emerging problem that requires new regulatory solutions. The FTC has been addressing manipulative design choices that harm consumers for decades under its Section 5 authority. Going forward, the boundaries of legality for commercial practices – whether in the digital or analog markets – should be guided by established doctrines of deception and unfairness, rather than through creating a new prescriptive, regulatory regime. This is particularly true for the United States, which has a rich history of protecting consumers through the flexibility of statutory authority and an evolving common law under the FTC rather than taking a prescriptive and overly broad regulatory approach.

---

[1] SIIA is the leading organization representing financial information, education technology, specialized content, information and publishing, and health technology companies. Our diverse membership of more than 700 companies and associations represent the broad and diverse landscape of the digital age. They provide services that are vital to our economic and social wellbeing; including helping learners of all ages prepare to succeed in their futures, managing the global financial markets, developing software that solves today's challenges, providing critical information that informs businesses large and small, and innovating for better health care and personal wellness outcomes. You can learn more about SIIA at www.siia.net.

Indeed, the FTC's enforcement history bears out that this approach works. An overview of the FTC's work over just the past ten years shows a rich enforcement history to combat design and marketing features that:

- steer users toward a particular course of action,[2]
- mislead consumers into registering for purported free trials of goods and services when actually enrolling consumers into undisclosed or poorly disclosed subscriptions with difficult to impossible cancellation features,[3]
- misrepresent privacy controls and software updates that result in expansive and inappropriate data collection practices,[4] and
- mislead consumers through undisclosed reviews/endorsements and other purportedly non-commercial content.[5]

Based on the FTC's body of law, developed both through Section 5 enforcement and set forth by specific frameworks like ROSCA and CAN-SPAM, it is unclear what new regulatory authority brings to the table other than the potential for duplicative and/or overreaching authority. The first is unnecessary. The second is dangerous.

Moreover, over-regulation of design choices beyond the FTC's existing authority will inevitably chill the truthful and accurate dissemination of commercial speech and trigger a potentially fatal conflict with the First Amendment. Regulatory authority that impedes the sharing of truthful and accurate information with consumers will collide with the First Amendment's free speech guarantees. While we appreciate that the workshop broached this topic, this issue warrants deeper consideration. If the FTC chooses to press forward with requests for new authority, it must carefully weigh the parameters of that within the confines of the First Amendment.

Focus Should Remain On Redressable Harms

As the FTC moves forward with its work on dark patterns, whether in the context of enforcement or pursuing a new regulatory framework, the focus should remain on consumer harm and identifying redressable harms. As was showcased during the workshop, the debate is still open regarding what does and does not constitute a

[2] *See* Appendix A
[3] *See* Appendix B
[4] *See* Appendix C
[5] *See* Appendix D

manipulative design. The FTC can influence and advance this debate by following its rich history of leveraging its authority to stop and remedy redressable consumer harms, whether in the context of advertising, marketing, privacy, or more generalized consumer protection matters. By focusing on redressable consumer harm, the FTC ensures that its resources are deployed to address patterns that are the most egregious and redressable.

Nagging Should Not Be Considered a Dark Pattern Except in Egregious Circumstances

During the workshop, Lior Strahilevitz suggested that "nagging" constitutes a dark pattern. He addressed this within the context of "[r]epeated requests for location access or updates [that] can wear consumers down. . . " We respectfully disagree and urge the FTC not to adopt an overly broad enforcement priority or to seek new regulatory authority to ban nagging without establishing clear guardrails to differentiate when a pattern of repeated requests is harmful and unlawful rather than necessary or even beneficial.

If nagging is defined as repetitive requests, for instance, it risks reaching notice and consent mechanisms that are required by law. SIIA's members support simplifying notice and consent mechanisms for consumers, wherever possible. But the regulatory reality is that many government-mandated frameworks require cumbersome mechanisms. Moreover, layered mechanisms may be the best way to provide notice and consent to provide consumers with access to full information. It is unfair to penalize companies for acting within the parameters of regulatory requirements or providing meaningful transparency by labeling any layered notice of consent mechanism as "nagging."

Many regulatory frameworks rely on notice and consent which burdens consumers rather than provide appropriate rules of the road to prevent privacy harms. Extending the dark patterns policy work to cover "nagging" is another example of the bad outcomes from over reliance on notice and consent; companies must navigate this structure within the confines of set regulatory parameters that may not best serve consumers and could create unnecessary confusion or conflicts around legal requirements, such as declaring a specific notice mechanism a dark pattern if it is necessarily repetitive. The United States should move forward with comprehensive, baseline privacy solutions that protect consumers and enable regulatory flexibility to provide just-in-time and layered notices.

Additionally, repetitive requests that risk being labeled as "nagging" often are a result of user-driven requests to access features that rely on data. For instance, many consumers prefer to only share their location data when it is necessary for a specific feature they are using on a smart device or browser. If the FTC determines that repetitive requests for consent are nagging, it risks taking away consumer choice and safeguards that actually limit data collection while empowering consumer choice.

Relatedly, many prompts that run the risk of the "nagging" label are actually beneficial to consumers because they are intended to prompt consumers to review account

settings, confirm their sharing decisions, or otherwise raise consumer awareness of the privacy controls available to them. These prompts should not be considered "nagging," or manipulative, or dark patterns.

Finally, prompts for users to make updates to their software are an essential security feature as these updates often patch vulnerabilities or address other security issues (as well as provide the latest version of features). Regular software updates are an important way to keep devices, and therefore users, secure. Designating such updates as "nagging," perhaps due to their frequency or other design aspects, might have the unint ended consequence of burdening and otherwise harming critical security infrastructure.

Future Actions Should Take Into Account the Value of the Features

We urge the FTC to use its expertise from decades of work in this area to ensure that any future enforcement actions or regulatory frameworks take into account that many design practices have intrinsic value to consumers and therefore should not be considered dark patterns as a per se rule. For instance, digital features like auto-play or content recommendations have been scrutinized. Yet these features are popular with consumers and hold value as consumers navigate their digital lives for both entertainment, education, and commercial purposes.

The Focus Should Be On Substantial Impact, Not Intent

If the FTC moves forward with seeking new regulatory authority, we urge it to focus on a framework that focuses on the substantial impact of patterns, rather than intent. First and foremost, this is aligned with the FTC's Section 5 authority which should be the bedrock for any new framework. Second, focusing on substantial impact provides a clear path forward in a space that is complex and layered. A focus on intent will be difficult for the FTC to enforce, but also difficult for companies to adhere to in a compliance program because it will depend on the individual motivations of designers rather than on outcomes. The better option is for the FTC to develop an effect or impact standard that can be measured objectively to ensure transparency, achievable, and fair outcomes.

Conclusion

We thank you again for this opportunity to provide our post-workshop comments.

Dated: May 28, 2021

Respectfully submitted,

/s/ *Sara C. DePaul*

Sara DePaul
Associate General Counsel & Senior Director, Technology Policy
SIIA - The Software & Information Industry Association
202-789-4471 Office / 614-439-4392 Mobile / @saracdepaul Twitter
siia.net/policy

Appendix A
Representative Examples of FTC Enforcement Actions Addressing Design Practices That Steer Users Towards a Particular Course of Action

1. **FTC v. Office Depot, Inc. & Support.com, Inc.** (Matter No. 172 3023) (2019): Enforcement action against Office Depot and its tech support firm that obtained more than $35 million in redress for unlawful practices that "tricked" consumers into buying computer repair and technical services with misrepresentations that a free virus scan had detected malware on consumers' computers. According to the complaint, the purported virus scan did not actually look for evidence of malware. Instead, it automatically told consumers that their system may be infected with malware if the consumers answered "yes" at any point during a series of questions regarding how their computer functioned. The complaint also alleged that the companies "aggressively pushed" the virus scan as a sales tool "despite complaints from store employees about the accuracy and reliability" of the program.

2. **FTC v. AH Media Group, LLC** (Matter No. 182 3047) (2019). Enforcement action alleging that the defendants used deceptive websites to trick consumers into free trials of beauty products when enrolling them in subscription plans by burying information about the continuity features and not requiring consumers to click to indicate their consent. The complaint alleged that the defendants buried the information "in small terms and conditions links, and in statements displayed in small font size and light-colored text that appear[ed] only after the consumer order[ed] a product." The FTC alleged that the defendants' practices made it difficult for consumers to cancel their subscriptions, and the company used "dummy websites" to fight chargeback requests that consumers made with their credit card companies.

3. **FTC. v. Nutraclick, LLC** (Matter No. X160052) (2016). Enforcement action in 2016 alleging a failure to disclose negative option features by burying the disclosures in dense terms and conditions language on the payments page next to distracting marketing text. When the defendants continued the conduct after the first case, the FTC brought separate enforcement action that required the company to pay 1.04 million, which represented the totality of consumer harm and resulted in a final order banning the company from negative option marketing.

4. **In re PaymentsMD, LLC** (Matter No. 132 3088) (2014). Enforcement action to stop a medical billing provider from misleading consumers into providing their personal health data using a design that made it difficult for consumers to read and understand a series of four authorizations for data collection while making it easy for consumers to skip over them while providing the data. Indeed, the FTC alleged that "[c]onsumers would reasonably believe that all four authorizations were being used to provide the Patient Portal billing services for which [the consumers] were registering." The FTC reached a settlement with PaymentsMD in 2015, which required the company to destroy any of the information it obtained using the flawed authorizations.

Appendix B
Representative Examples of FTC Enforcement Actions Involving Misleading Claims of "Free" Trials to Trick Consumers Into Enrolling Into Subscription-Based Memberships That Are Difficult Or Impossible to Cancel

1. **FTC v. Age of Learning, Inc., d/b/a ABCmouse.com** (Matter No. 172 3186) (2020). Recent enforcement action alleging that the company misled consumers with offers of a trial membership that enrolled them into paid memberships that were renewed indefinitely following the trial period. The FTC alleged that despite claiming to have "easy cancellation" procedures, the company in fact made it incredibly difficult for subscribers to cancel their memberships. Indeed, the FTC noted that cancelling was so cumbersome that "[o]ver the course of at least three years, hundreds of thousands of consumers who visited . . . [the] cancellation path . . . remain enrolled." The company settled the FTC charges and agreed to pay $10 million in consumer redress.

   Notably, Commissioner Chopra issued a separate statement in which he explicitly referenced the defendants' practices as dark patterns. He called on the FTC to combat unlawful dark patterns with the "numerous tools [it has] to root out the kinds of tricks and traps we saw in this matter." He specifically pointed to the FTC Act as a tool, stating that it "vests the Commission with authority to analyze emerging practices and define which practices are unlawful." Importantly, the statement neither identified any business practices the FTC cannot address with its existing arsenal, nor any harms that went unremedied in the case. Instead, it would appear the FTC is facing a question of enforcement discretion and prioritization rather than lack of authority.

2. **FTC v. Triangle Media Corporation** (Matter No. 172 3108) (2018). Enforcement action against online marketers that used advertisements to direct consumers to websites that offered "RISK FREE" trials for skin creams, e-cigarettes, and dietary supplements. Despite these claims, consumers were charged nearly $100 for their first shipment and then enrolled into a negative option continuity plan without their consent. To perpetuate the scheme, the defendants sent consumers deceptive order confirmation mails that omitted these additional charges. They also made it difficult for consumers to cancel their subscriptions. The FTC was able to obtain orders for equitable monetary relief that resulted in the agency sending redress checks totaling more than $8.7 million to harmed consumers.

3. **FTC v. Bunzai Media Group, Inc. (AuraVie)** (Matter No. X150047) (2015). Enforcement action against seven individual and 15 companies alleging consumers were misled and harmed through online advertisements that offered purported "risk free" trials but enrolled consumers in subscription plans with high recurring fees. The FTC alleged that the companies made it incredibly difficult for consumers to cancel by refusing to process cancellation requests, refusing to issue refunds, denying returns even when done in accordance with the defendants' policies, and often only granting cancellation requests if the consumer escalated the issue by complaining to their credit card companies, state regulatory authorities, or the BBB. The FTC was able to send more than $1 million in refunds to consumers.

Appendix C
Representative Examples of FTC Enforcement Actions Addressing Deceptive Claims Regarding Privacy Controls and Software Updates

1. In re Tapjoy, Inc. (Matter No. 172 3092) (2021). Enforcement action brought just earlier this year alleging that a mobile advertising company deceived users into "divulg[ing] personal information [to] or spend[ing] money [on]" third-party services by promising users in-game virtual currency as a reward, which the company then often did not provide. The FTC alleged that the company made it difficult for users who were owed in-game virtual currency to contact the company regarding the outstanding regards. Moreover, after receiving "hundreds of thousands of complaints from consumers who said they never received their promised rewards," the company also allegedly implemented a policy of prohibiting users from submitting complains within 24 hours of interacting with advertising partners. The FTC and Tapjoy agreed to a settlement order that requires the company to stop these ongoing unlawful behaviors and to investigated claims from defrauded users.

2. In re Zoom Video Communications, Inc. (Matter No. 192 3167) (2020). Another recent enforcement action resolving allegations that Zoom misled users into installing a software update with claims that it would fix minor bugs when in reality it did much more, including installing a locally hosted web server that "would circumvent a Safari browser privacy and security safeguard," remained on users computers even if they deleted the Zoom app, and automatically re-downloaded and re-installed the app if a user deleted the Zoom app but later clicked on a Zoom link. Under a settlement order with the FC, Zoom is required to implement security standards and to submit to certain ongoing monitoring and reporting, among other things.

3. In re Paypal, Inc. (Matter No. 162 3102) (2018). Enforcement action that Paypal misled Venmo users about the app's privacy controls, including by creating a difficult to parse set of privacy settings that required users to change their default audience setting and transaction sharing settings to keep their in-app transactions private. The complaint alleged that the default audience setting included a label that "would lead a reasonable consumer to believe that she could limit the visibility of all other future transactions by restricting this setting," when in reality the consumer had to also change a second setting (called the transaction sharing setting) to ensure that the transactions remained private. The FTC alleged that this overrode the consumer's "clearly expressed privacy preferences." The company agreed to a settlement order.

4. FTC v. Frostwire, LLC and Angel Leon (Matter No. 112 3041) (2011). The FTC alleged that a file-sharing software developer misled consumers about which files on their computers would be shared publicly. The complaint focused on the Frostwire Setup Wizard, which prompted consumers to click through a number of dialogue boxes in order to install the software. One such dialogue box was entitled "Save Folder and Shared Folders" and allegedly gave users the impression that "files stored in the 'Shared' folder would be shared with the file-sharing network" and "files stored in the 'Save' folder would not be shared with the file-sharing network." The complaint further alleged that the Setup Wizard asked users to "choose a folder where you would like your files to be downloaded. You can also choose folders you would like to share with other users

running Frostwire." Frostwire allegedly did not disclose to users that "any files subsequently downloaded using the application would, by default, be shared as 'Individually shared' files even if they were not saved to a 'Shared' folder." The FTC reached a settlement with Frostwire which, among other things, barred the company from continuing to use confusing default settings to share consumers' files and required Frostwire "to provide free upgrades to correct the unintended sharing."

Appendix D
Examples of Representative Enforcement Actions For
Misleading Reviews/Endorsements and Other Purported Non-Commercial Content

1. In re Sunday Rile Modern Skincare, LLC & Sunday Riley (Matter No. 192 3008) (2019): Enforcement action against the skincare company Sunday Riley and its CEO alleging that the company maintained an official policy of directing employees to create fake profiles and post fake reviews touting the company's products on third party websites. The FTC also alleged that once the fake reviews were identified and removed, the company doubled down on its scheme by instructing employees to use a VPN to shield their IP addresses when posting additional fake reviews. The company and its CEO reached a consent decree with the FTC that settled the FTC's charges and prohibited the company and its employees from posting reviews of its products.

2. FTC v. Match Group, Inc. (Matter No. 172 3013) (2019). Enforcement action that the Match Group, the owner of a number of dating websites and apps, deceived non-paying subscribers into paying for subscriptions through advertisements that touted fake romantic interests. The FTC also alleged that Match misled non-paying subscribers to update their subscription with promises of a trial period along with a "guarantee" that the trial would be free if they did not "meet someone special" during the trial period. The FTC alleged, however, that the company did not properly disclose to users that they would need to meet certain eligibility criteria to benefit from the guarantee. Lastly, the FTC alleged that the company made it difficult for users to cancel their subscriptions by implementing a process that even the company's employees described as "hard to find, tedious, and confusing." This matter remains pending in federal district court.

3. In re Practice Fusion, Inc. (Matter No. 142 3039) (2016). Enforcement action against a cloud-based EHR company that created an online directory of providers and then populated the director with revies by emailing the patients of providers who used the EHR software and claiming to solicit the feedback to improve their patient service. The emails were signed as the patient's providers and falsely indicated that the information as requested on behalf of the provider. The company, however, posted the written feedback publicly online even when it contained the patient's personal health information. The company settled its charges with the FTC, agreeing to make changes including obtaining users' express consent before sharing their information publicly in the future.