



Bringing Dark Patterns to Light: An FTC Workshop

**comments from the
Network Advertising Initiative (NAI)**

**filed with the
Federal Trade Commission**

March 15, 2021

The Network Advertising Initiative (NAI) appreciates the opportunity to provide comments on the Federal Trade Commission’s (“FTC” or “Commission”) upcoming virtual workshop “Bringing Dark Patterns to Light,” and we look forward to attending the workshop and using the dialogue to inform our further thinking on this topic.

Summary

At a time when Americans are spending more time than ever on connected devices, this discussion about “dark patterns” is important and timely. While there are different definitions of this term, and even various taxonomies to compare and contrast specific practices,¹ dark patterns are generally defined as techniques intentionally used to mislead or manipulate users, obscuring, subverting or impairing consumer autonomy, decision-making, or choice. An implication of this common definition is that the end result of the manipulation is a harmful or undesirable outcome for the user. As the Commission considers the complex issue of dark patterns and user interfaces (UI) more broadly, it is essential to draw a clear line between practices that harm consumers, and those that are little more than a nudge seeking to achieve a business purpose, particularly where such purpose is consistent with the objectives and preferences of its users. Such practices can be analogous to those in the physical world, product placement by a retailer to promote certain products over others. In these comments, we also explore the so-called “light” or “bright” patterns, which pose their own unique challenges for both users and regulators.

The NAI appreciates the Commission’s intention to focus the upcoming workshop primarily on those practices with the most harmful outcomes, such as sites that sneak extra items into a consumer’s online cart, to require users to navigate a maze of screens and confusing questions to avoid being charged for unwanted products, or deceptively tricking users into unnecessary purchases. However, given the expertise and experience of the NAI, these comments focus narrowly on the assessment of potential dark patterns that are relevant to the digital advertising industry and the “notice and choice” framework for digital collection of consumer data.

As we highlight below, the NAI is committed to maximizing the efficiency and effectiveness of the notice and choice framework within the digital advertising marketplace, and to enabling users to make informed decisions—both initially and with persistence—about the use of their data for advertising purposes. In summary, these comments make the following key points:

1. The NAI has a history of establishing industry-leading guidelines to maximize the effectiveness of the notice and choice framework for consumers, enabling them to make informed decisions about the use of their data for advertising purposes, and we are well positioned to promote best practices for UIs that make it easy for users to exercise privacy choices.
2. The FTC has substantial authority under Section 5 of the FTC Act to protect consumers against deceptive and unfair practices, including those that might be characterized as dark patterns.
3. Avoiding dark patterns and actively seeking to maximize efficiency and clarity can help to offset *some* of the inherent challenges posed by the notice and choice framework, but the best solution is to minimize reliance on the framework altogether.
4. Regulators assessing potential dark patterns should refrain from dictating specific practices or erecting limitations on the ability of businesses to effectively communicate with their users.

¹ Hartzog, Woodrow. *Privacy's Blueprint: The Battle to Control the Design of New Technologies*. Harvard University Press, 2018.

5. “Light patterns” should only seek to advance users’ ability to make informed choices, not shape markets and business models.
6. Contrary to developing a prescriptive new regulatory framework, the right approach is to increase education and promote self-regulation around these practices.

About the NAI

NAI is the leading self-regulatory organization dedicated to responsible data collection and use by advertising technology companies engaged in Tailored Advertising and Ad Delivery and Reporting (ADR)² in the United States. The NAI, a non-profit self-regulatory organization and trade association, was formed in 2000 and has over 100 member companies, each of which is required to adhere to the strong digital advertising best practices set forth in the NAI Code of Conduct (“Code” or “NAI Code”), which the NAI enforces through annual compliance reviews, and which implements stringent consumer privacy protections. The Code is rooted in the widely accepted Fair Information Practice Principles (FIPPs)³, and it applies those principles to the digital advertising ecosystem by, among other things, instituting robust notice and choice requirements and restrictions on the use and sharing of data. The Code heightens restrictions and requirements for more sensitive data types. For example, the collection and use of Precise Location Information requires Opt-In Consent accompanied by detailed, just-in-time notice about the collection, use, and sharing of such information.

1. The NAI has a history of establishing industry-leading guidelines to maximize the effectiveness of the notice and choice framework for consumers, enabling them to make informed decisions about the use of their data for advertising purposes, and we are well positioned to promote best practices for UIs that make it easy for users to exercise privacy choices.

Since its inception, the core objective of the NAI has been to guide the digital marketplace on matters of consumer transparency. We believe that consumers should be able to make decisions about the use of their data and to efficiently communicate their decisions, either by opting-in or opting-out, depending on the sensitivity of the data. NAI staff works with members, both during onboarding and annual compliance reviews, to help ensure that disclosures are complete, clear, and easy to find. This includes

² Tailored Advertising is defined by the NAI Code as 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.” Ad Delivery and Reporting is “separate and distinct from Tailored Advertising, and 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, including, but not limited to: providing a specific advertisement based on a particular type of browser, device, time of day, or real-time precise location; statistical reporting, traffic analysis, analytics, optimization of ad placement; ad performance, reach, and frequency metrics (including frequency capping); sequencing of advertising creatives; billing; and logging the number and type of ads served on a particular day to a particular website, application or device. ADR does not include data collection and use for security and fraud prevention.” See Network Advertising Initiative, 2020 NAI Code of Conduct § I.A, I.Q (2020), https://www.networkadvertising.org/sites/default/files/na_i_code2020.pdf [hereafter 2020 NAI Code of Conduct].

³ See Fed. Trade Comm’n, Privacy Online: A Report to Congress 7 (1998), <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf>; see also Fed. Trade Comm’n, Privacy Online: Fair Information Practices in the Electronic Marketplace (2000), <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf>.

requirements for direct consumer choice links, enhanced notice, and various disclosure requirements, including relevant disclosures tied to health and political advertising.

The NAI is also actively working to set a high standard across the industry for how location and other sensitive data may be used for advertising purposes. Under the NAI Code, the following data types require Opt-In Consent prior to their use for Tailored Advertising or Ad Delivery and Reporting purposes: Precise Location Information, Sensitive Information (which includes sexuality and sensitive health-related data), Personal Directory Information, and Sensor Information (cameras, microphones, or other sensors that may collect biometric data from a device). In addition, users from whom Opt-In Consent is obtained must have access to detailed notice of the intended uses of such data, including data sharing.

In connection with this requirement, the NAI released guidance⁴ for its members, clarifying the Code's requirement to provide notice when obtaining Opt-In Consent for those enumerated categories. The guidance seeks to ensure that users being asked to consent for the use of their data, including Precise Location Information, understand how their data is being used and with what types of parties the data will be shared. Together, the NAI's Code requirements, guidance, and best practices give clarity to members on how to provide relevant and timely information to a consumer, and how to implement efficient processes to grant or revoke consent.

In light of recent concerns raised about dark patterns, the NAI is assessing existing practices and related research pertaining to various UIs, with the goal to promote industry best practices to avoid dark patterns across digital advertising. Observing approximately one hundred companies' disclosures and consent mechanisms, NAI staff is uniquely positioned to enforce requirements and to promote best practices for making disclosures and consumer choices more prominent and easier to understand. This can range from font and background color, to the size of a link, to the amount of clicks necessary to access information. As discussed in greater detail below, the NAI supports the adoption of a framework whereby the Commission provides a regulatory backstop for the NAI and other similarly positioned organizations to address dark patterns through self-regulation.

2. The FTC has substantial authority under Section 5 of the FTC Act to protect consumers against deceptive and unfair practices, including those that might be characterized as dark patterns.

Given that dark patterns are essentially a modern form of deceptive or unfair trade practices, the Commission is well equipped to apply its foundational authority under Section 5 of the FTC Act to enforce against these activities. The recent FTC enforcement action against Age of Learning, Inc. is an example of this reality. In the action, the Commission exercised its Section 5 authority, in conjunction with the Restore Online Shoppers Confidence Act (ROSCA), to enforce against deceptive and unfair practices referred to as a "Dark pattern trap," where billing practices and subscription cancellation combined to present a situation that was both misleading and manipulative.⁵

In a separate concurring statement to that case, Commissioner Rohit Chopra made it clear that these unlawful practices constitute "dark patterns" and that, "[t]he FTC has numerous tools to root out the

⁴ See Guidance for NAI Members: Opt-In Consent (2019), https://www.networkadvertising.org/sites/default/files/final_nai_optinconsent-guidance19_final.pdf.

⁵ In re Age of Learning, Inc., Federal Trade Commission, 17 Sept. 2020, www.ftc.gov/enforcement/cases-proceedings/172-3186/age-learning-inc-abcmouse.

kinds of tricks and traps we saw in this matter.”⁶ He specifically pointed to the FTC Act as a tool, because it prohibits unfair and deceptive practices, “and vests the Commission with authority to analyze emerging practices and define which practices are unlawful.”⁷ Commissioner Chopra urged the Commission to “deploy these tools to go after large firms that make millions, or even billions, through tricking and trapping users through dark patterns.”⁸ The NAI concurs that the Commission is well equipped to engage in such enforcement, and that this represents a practical enforcement priority in the months ahead. Notably, neither Commissioner Chopra’s statement nor the consent order identified any enforcement limitations facing the Commission with respect to business practices that need to be reigned in. Neither provide a case for expanding the FTC’s authority to make regulations beyond its current deceptive and unfairness authority.

Recent research examines the issue the Commission is seeking to explore, the application of current legal frameworks in which federal and state agencies can bring an enforcement action against dark patterns. According to the authors, “[m]any dark patterns appear to violate federal and state laws restricting the use of unfair and deceptive practices in trade.”⁹ For example, the authors identify several dark pattern cases brought under the deceptive prong of § 5 of the FTC Act despite not describing them as “dark patterns.”¹⁰

Prominent examples include a loan company that made a costly repayment option as the default and buried the information to switch to a different option in long, “densely packed text,”¹¹ online advertising that was disguised as a news article and presented false reviews,¹² Office Depot “falsely informing consumers that their computers were infected with malware and then selling them various ... malware removal services they did not need,”¹³ and a company that included fine print on the back of a personal check indicating “that by cashing the check[,] the consumers were signing up for a monthly subscription...to an internet access service.”¹⁴ Since § 5 of the FTC Act does not require an intent to deceive and rather, examines whether “the ‘overall net impression’ of the defendant’s communication is misleading.” These examples demonstrate that dark pattern cases, which steer a large number of consumers into acquiring a service they do not want, can be regulated as deceptive trade practices.¹⁵

As for the unfairness prong of § 5 of the FTC Act, the authors note that case law is “less clear.”¹⁶ The current test requires three elements: the trade practice (1) “causes or is likely to cause substantial injury to consumers”; (2) “is not reasonably avoidable by consumers themselves;” and (3) “is not outweighed by countervailing benefits to consumers or competition.”¹⁷ The second prong prohibits “practices that

⁶ Chopra, Rohit. “Regarding Dark Patterns in the Matter of Age of Learning, Inc.” Federal Trade Commission, 2 Sept. 2020, www.ftc.gov/system/files/documents/public_statements/1579927/172_3086_abcmouse_-_rchopra_statement.pdf.

⁷ *Ibid.*

⁸ *Ibid.*

⁹ Jamie Luguri & Lior J. Strahilevitz, *Shining a Light on Dark Patterns*, at Abstract.

¹⁰ *Id.* at 30.

¹¹ *Id.* at 31 (quoting *FTC v. AMG Capital Management*, 910 F.3d 417 (9th Cir. 2018)).

¹² *Id.* at 32 (quoting *FTC v. LeadClick Media, LLC*, 838 F.3d 158 (2d. Cir. 2016)).

¹³ *Id.* at 32-33 (quoting *FTC v. Office Depot, Complaint for Permanent Injunction and Other Equitable Relief*, Case No. 9-19-cv-80431 (S.D. Fla. Mar. 27, 2019)).

¹⁴ *Id.* at 34 (quoting *FTC v. Cyberspace.com, LLC*, 453 F.3d at 1196 (9th Cir. 2006)).

¹⁵ *Id.* at 30.

¹⁶ *Id.* at 34.

¹⁷ *Id.* at 34 (quoting *FTC Policy Statement on Unfairness*, 104 FTC 949 (1984)).

prevent consumers from effectively making their own decisions,” largely because the danger is not obvious and consumers are not “aware of the possible risk.”¹⁸ The third prong requires a “cost-benefit analysis” that examines business costs, consumer benefit, societal burdens, and public policy considerations.¹⁹ Luguri & Strahilevitz conclude that the “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.”²⁰

3. Avoiding dark patterns and actively seeking to maximize efficiency and clarity can help to offset some of the inherent challenges posed by the notice and choice framework, but the best solution is to minimize reliance on the framework altogether.

A guiding objective for the NAI over the years has been to encourage companies to provide timely and persistent opportunities for users to learn about the use of their data for advertising purposes, and to opt-out or opt-in based on that knowledge. However, extensive research and debate around the notice and choice framework have revealed that it suffers from multiple inherent challenges, all of which can contribute to user frustration, uninformed decision-making, and even indifference or fatigue from over-notification. Our years of experience reviewing member practices and engaging in discussions with policymakers, researchers, privacy advocates and other stakeholders reveals that clear, easy to understand UIs are vital to providing proper notice and choice, but they can also be quite challenging to get right.

First, providing privacy notices that are sufficiently descriptive, yet succinct, regarding varying consumer data uses, is not a trivial exercise. This is compounded by the reality that while some users actively prefer to know more about what type of data is collected from them, and control over whether and how the data is used, others have less interest in managing their data sharing practices, or feel that it is something they are not well equipped to do.²¹ Of course, all businesses also strive to enable users to access digital content and services as efficiently as possible, with little distraction or deterioration in user experience. In most cases, well-intentioned UIs are therefore designed to balance the need to maximize transparency and user control with the goal of ensuring consumers can move effortlessly to the digital content they are seeking without being bogged down by reading disclosures or making forced choices.

Second, informing users about the value exchange presented by data-driven advertising is essential, because consumers generally lack awareness but have come to expect and demand free or low-cost digital content and services.²² When it comes to accessing digital media, 74 percent of consumers will

¹⁸ *Id.* at 35.

¹⁹ *Id.* at 35.

²⁰ *Id.* at 37.

²¹ Auxier, Brooke, et al. “Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information.” *Pew Research Center: Internet, Science & Tech*, Pew Research Center, 17 Aug. 2020, www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

²² NAI’s 2019 consumer survey revealed that nearly 60% of respondents prefer their online content to be paid for by advertising, while another question sought feedback from consumers on how much they currently pay for online content and how much they would be willing to pay. Nearly 90% said they are unwilling to pay a significant amount of money to continue receiving apps and online content that they currently receive for free. The survey provided a strong affirmation that the ad-supported content model is ideal for most consumers. See, [Blog | NAI](#).

only download an application if it's free and 51 percent of consumers will only download music if it's free."²³ Indeed, ad-supported digital content and services have been an essential element of the rich digital media ecosystem developed over the last several decades. Advertising subsidizes the content and services Americans expect and rely on, including video, news, music, and more, and underwrites the creation of innovative apps and technologies that connect individuals and businesses.

Third, over-notification is itself a problem that inherently places responsibility on the user to make decisions that are not simple. The NAI and others have repeatedly warned against the negative impact of over-notification, and recent empirical research on the role of privacy fatigue in affecting online privacy behavior found that privacy fatigue has a stronger impact on privacy behavior than privacy concerns do.²⁴ Users experiencing privacy fatigue put less effort into making privacy decisions, and they may demonstrate disengagement behavior due to emotional exhaustion and cynicism.²⁵

While this research does not directly relate to dark patterns in the consent process, it presents a highly relevant perspective when assessing differing objectives of UIs for user consent notices. The increased frequency of opt-in requirements for access to a users' data cannot be an effective model, regardless of a particular UI seeking to simplify the process—ultimately it is a complex and inefficient process with little practical benefit in most cases.

Importantly, the Commission and other policymakers could maximize the benefit to consumers by not only enforcing against the deceptive and unfair choice mechanisms, but by adopting public policy alternatives that lessen the reliance on the model altogether. To that end, the NAI is a founder and leading member of the Privacy for America coalition, which urges adoption of a federal law that requires data-driven businesses to implement strong data protection and privacy practices, and to prohibit a set of unreasonable data practices, rather than placing the burden on consumers from whom data is collected.²⁶

4. Regulators assessing potential dark patterns should refrain from dictating specific practices or erecting limitations on the ability of businesses to effectively communicate with their users.

The Commission and state enforcement officials should continue to provide education and enforcement against misleading, deceptive and unfair practices associated with the provision of notice and choice, but they should not seek to develop prescriptive requirements that could further undermine an already challenged framework.

California Attorney General Xavier Becerra recently proposed modifications to the California Consumer Privacy Act (CCPA) regulations that would have this adverse effect. Specifically, the proposed

See also [Zogby Analytics Public Opinion Survey on Value of the Ad-Supported Internet](#), Commissioned by the Digital Advertising Alliance (May 2016)

²³ "Consumer Preferences Shift to Digital Content Reveals Limelight Networks' New 'State of Digital Downloads' Report." Consumer Preferences Shift to Digital Content Reveals Limelight Networks' New 'State of Digital Downloads' Report | Business Wire, 13 June 2017, www.businesswire.com/news/home/20170613005548/en/Consumer-Preferences-Shift-to-Digital-Content-Reveals-Limelight-Networks%E2%80%99-New-%E2%80%98State-of-Digital-Downloads%E2%80%99-Report.

²⁴ Hanbyul Choi, Jonghwa Park, & Yoonhyuk Jung, *The Role of Privacy Fatigue in Online Privacy Behavior*, Computers In Human Behavior (2018), <https://doi-org.proxygw.wrlc.org/10.1016/j.chb.2017.12.001>.

²⁵ *Id.* at 48.

²⁶ See Privacy for America Coalition policy principles, at <https://www.privacyforamerica.com/overview/>.

modifications would prohibit a business from requiring a consumer “to click through or listen to reasons why they should not submit a request to opt-out *before* confirming their request.”²⁷ While minimizing unnecessary distractions and encouraging fair and efficient opt-out processes are practical goals, this restriction creates an inappropriate limitation on businesses’ ability to communicate with their consumers, and it possibly infringes on businesses’ First and Fourteenth Amendment right to commercial speech.

As the research cited above confirms, consumers have continually expressed their preference for ad-supported digital content and services, but they generally lack a clear understanding of the current data-driven advertising support model. For instance, local news publishers continue to struggle to get readers to pay subscription fees for their content, even though this content is highly valuable to consumers and society. Thus, most news publishers have become increasingly reliant on tailored advertising, because it provides greater revenue than traditional advertising.²⁸ Therefore, limits on consumers’ receipt of factual, critical information about the nature of the ad-supported Internet would actually undermine a consumer’s ability to make an informed decision. A business should be able to provide a reasonable notice to consumers about the benefit that data-driven advertising provides as a critical source of its revenue.

Although thoughtful UIs and careful, clear wording could help to minimize the annoyance or inconvenience of such practices, regulations should not prevent consumers from receiving and businesses from providing full, fair, and accurate information during the opt-out process, particularly regarding important information about their privacy choices, such as information about the vital nature of the ad-supported Internet.

5. “Light patterns” should only seek to enhance users’ ability to make informed choices, not shape markets and business models.

Within the discussion around Dark Patterns is a somewhat newer term; the concept of “light patterns,” sometimes also referred to as “bright patterns.” These terms are generally used to describe practices that make it easy for users to navigate, read, and follow directions or make choices in general. Such UIs are laudable and exemplary of businesses seeking to do right by their users. An alternative definition of a light pattern represents practices that make proactive decisions on behalf of users, having their best intentions in mind.²⁹ However, the “best intention” of a consumer is not uniform. Therefore, light patterns that go beyond striving to ease user navigation and decision-making and make assumptions for consumers, about what is in their best interest, should be approached cautiously. As discussed above, the majority of users prefer ad-supported digital content, apps and services. So, a business practice or UI that *assumes* that advertising, particularly data-driven advertising, is not in the best interest of consumers, fails to contemplate negative market externalities to such consumers, including that less reliance on data-driven advertising could result in an increase in fee-based digital content and apps - an outcome contrary to their stated preferences.

²⁷ See California Department of Justice, *Notice of Fourth Set of Proposed Modifications to Text of Regulations and Addition of Documents and Information to Rulemaking File* (Dec. 10, 2020), <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-notice-4th-set-mods.pdf>.

²⁸ Beales, Howard, and Eisenach, Jeffrey, *An Empirical Analysis of the Value of Information Sharing in the Market for Online Content*, commissioned by the Digital Advertising Alliance (January 2014).

²⁹ Coleman, Aidan. “Light and Dark UX Patterns.” Medium, Prototypr, 26 May 2019, blog.prototypr.io/light-and-dark-ux-patterns-19ffcaa50e9a.

Further, different business revenue models complicate the consideration of dark and light patterns even further. For instance, Apple and Google are the two major mobile smartphone operating system providers, with very different revenue models. It is widely recognized that Google maintains a heavily ad-supported business, with data-driven advertising fueling its cutting-edge services, ranging from search to content streaming, to apps and other services. It is less widely recognized that Apple has a distinctly different business model, relying very little on advertising revenue and instead seeking to generate more revenue from user fees, subscriptions and commissions from partners based on fees that apps charge their users directly.³⁰ If fewer consumers opt-in to the use of anonymous data from their apps to support advertising and marketing, app developers will likely be forced to charge consumers for their apps, as well as in-app content, to offset lost advertising revenue.

While a consumer may prefer not to participate in data-driven advertising, with all outcomes being equal, it is vital that they be able to make an informed decision, particularly when that decision may promote a shift to a fee-based ecosystem where apps come at a cost to them. Therefore, Apple's policies that promote user privacy also present a unique business opportunity for them. Recently adopted practices by Apple are exemplary of this. The word "tracking" is used very broadly, and publishing app terms of service possibly prevent publishers from collecting user data on their own app if the user doesn't opt-in to "tracking" on the iOS platform, regardless of whether a user has already consented to the use of their data for advertising. These practices could quite likely lead to an increase in the adoption of fee-based apps, which would directly increase revenue for Apple.³¹

Requiring an opt-in for consumer data use for tailored advertising is a very legitimate decision for any technology company or digital business to make. However, this example highlights the complexity of what may or may not be in a users' "best interest," and therefore what may or may not constitute a "light" or "dark" pattern.

6. Contrary to developing a prescriptive new regulatory framework, the right approach is to increase education and promote self-regulation around these practices.

The Commission has long played a valuable role in helping to educate consumers and market participants about certain practices, with the goal of enhancing consumer confidence and protecting against bad actors. A relevant example is the Admongo.gov campaign launched by the Commission to educate children (ages 8-12) about advertising and help them make informed consumer decisions as they play an active role in family purchases.³² This is a helpful campaign to boost advertising literacy by raising awareness of advertising and marketing messages, teaching critical thinking skills that will allow tweens to better analyze and interpret advertisements, and demonstrating the benefits of being an informed consumer. Admongo.gov serves as a good example of creative educational opportunities that

³⁰ Strategist, Aparna Growth. "3 Ways Apple Makes Money From The iPhone." MobileAppDaily, MobileAppDaily, 6 May 2019, www.mobileappdaily.com/how-apple-makes-money-from-iphone#:~:text=The%20popularity%20of%20the%20App,made%20through%20the%20App%20Store.

³¹ Freund, Leigh. "Requiring App-by-App Opt-in for Personalized Ads Will Confuse Consumers, Harm Developers, and Benefit Apple." Network Advertising Initiative, 23 June 2020, http://www.networkadvertising.org/sites/default/files/press_release-requiring_app-by-app_opt-in_for_personalized_ads.doc.pdf.

³² "Federal Trade Commission." | Admongo.gov, www.consumer.ftc.gov/Admongo/about.html.

the Commission could engage in, particularly if they were provided with a larger budget for such activities.

As the leading self-reg industry association for digital advertising, the NAI is also strongly supportive of efforts by the Commission and other policymakers to leverage self-regulation to incentivize companies who actively seek to uphold high privacy standards. As a leading member of the Privacy for America coalition, the NAI is a proponent of a national privacy framework that encourages the development of certification programs by qualified organizations that could be granted approval to develop rigorous standards and best practices, and to provide robust oversight of participating organizations.³³ The NAI believes that such a self-regulatory—or co-regulatory—framework, with the FTC serving as a backstop, could be very effective in providing for best practices surrounding UI for various online business models. Even in the absence of federal legislation that formalizes and provides oversight for promotion of consumer privacy practices, the Commission could empower to the NAI and other leading self-regulatory organizations with practical enforcement guidance around certain practices that are deceptive or unfair.

Conclusion

Again, thank you for the opportunity to provide input into this process. The NAI looks forward to virtually attending the workshop and providing additional input as the Commission further considers the key questions identified by the workshop notice, and additional issues raised during the workshop.

³³ See Privacy for America Coalition policy principles, FTC-Approved Certification Programs at <https://www.privacyforamerica.com/overview/principles-for-privacy-legislation-dec-2019/#certification> (“To enhance compliance and provide flexibility where needed, the framework would encourage the development of certification programs by qualified organizations. If a program receives and maintains approval from the FTC, member companies that adhere the program’s requirements would be presumed to be compliant with the law. To ensure robust consumer protections, these programs would be required to include rigorous standards and oversight of member companies, including clear rules of conduct, public attestations of compliance by the companies, mandatory audits, meaningful disciplinary action for non-compliance, and annual reports to the public.”).