CENTER FOR INFORMATION TECHNOLOGY POLICY
PRINCETON UNIVERSITY

August 2, 2022

Via Regulations.gov
Before the
Federal Trade Commission
Washington, D.C.

Digital Advertising, P114506

Thank you for the opportunity to submit comments on the Federal Trade Commission's update of the 2013 version of its online digital advertising guidelines ("Disclosure Guidelines"). The undersigned are a group of interdisciplinary academic researchers with backgrounds in computer science, information science, law, and communications who have extensive expertise studying online behavior and consumer deception.[1] We write to offer suggestions on how the Commission might update the Disclosure Guidelines to account for the ways current and emerging technologies might take advantage of consumers.

At the outset we commend the Commission for focusing on the growing problem of "dark patterns," also known as "manipulative designs." Businesses can use dark patterns in their online choice architecture (options presented to consumers)[2] to engage in unfair or misleading practices.[3] We support the

[1] The Comment is coordinated by Dr. Jennifer King (Stanford Institute for Human-Centered Artificial Intelligence) and Princeton CITP's Technology Policy Clinic, which provides nonpartisan research, analysis, and commentary to policy makers, industry participants, journalists, and the public. These comments reflect the independent views of the undersigned scholars.
[2] See https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patters_paper.pdf
[3] E.g., Kerstin Bongard-Blanchy et al., *"I am Definitely Manipulated, Even When I am Aware of it. It's Ridiculous!" - Dark Patterns from the End-User Perspective*, ACM DIS (2021); U.K. Competition and Markets Authority, Online Choice Architecture: How Digital Design Can Harm Competition and Consumers (2022). available at:

Commission's efforts to provide guidance to businesses on avoiding dark patterns in their interactions with consumers.

As documented in several research studies, consumers may encounter dark patterns in many online contexts, such as when making choices to consent to the disclosure of personal information[4] or to cookies,[5] when interacting with services and applications like games or content feeds that seek to capture and extend consumer attention and time spent,[6] and in e-commerce,[7] including at multiple points along a purchasing journey.[8] Dark patterns may start with the advertising of a product or service, and can be present across the whole customer path, including sign-up, purchase, and cancellation. As a result, the Commission's guidance should cover the business's entire interaction with the consumer to ensure that they are allowed to engage in free and informed transactions. And, as we explain in further detail below, the guidance needs to squarely address the challenge that providing

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1066524/Online_choice_architecture_discussion_paper.pdf.

[4] Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. 2016. Tales from ¨ the dark side: Privacy dark strategies and privacy dark patterns. Proceedings of the Privacy Enhancing Technologies, 4 (2016), 237–254.

[5] The aspect of privacy is particularly salient. For research on information and personal data, see Than Htut Soe et al., "Circumvention by Design - Dark Patterns in Cookie Consent for Online News Outlets," *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*, 2020, https://doi.org/10.1145/3419249.3420132.

[6] Ibid.

[7] Jennifer Valentino-DeVries, "How e-Commerce Sites Manipulate You into Buying Things You May Not Want," The New York Times (The New York Times, June 24, 2019), https://www.nytimes.com/2019/06/24/technology/e-commerce-dark-patterns-psychology.html.

[8] For a summary of contemporary literature on dark patterns, see: Arunesh Mathur, Jonathan Mayer & Mihir Kshirsagar, *What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods*, ACM CHI (2021) as well as Alessandro Acquisti et al., "Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online," *ACM Computing Surveys* 50, no. 3 (2018): pp. 1-41, https://doi.org/10.1145/3054926.

additional disclosures, standing alone, will not cure the harms caused by a number of dark patterns.

1. The revised guidance document should address the use of dark pattern techniques in digital advertising. (Question 1)

Dark patterns are user interface techniques that benefit an online service by leading consumers into making decisions they might not otherwise make.[9] Some dark patterns deceive consumers, while others exploit cognitive biases or shortcuts to manipulate or coerce them into choices that are not in their best interests. While behavioral researchers have studied the psychology of deceptive persuasion in the marketplace for decades,[10] the advent of the Internet has spurred a growing number of academic studies on how online services can use digital interfaces to manipulate consumers in a variety of different settings.[11] In the context of online interfaces, the term "dark patterns" was coined in 2010 by Harry Brignull (a user experience designer who created the website darkpatterns.org[12]) to spotlight interface designs that he described as "tricks used in websites and apps

[9] Definitions of the term "dark pattern" vary, sometimes in subtle ways. *See* Arunesh Mathur, Jonathan Mayer & Mihir Kshirsagar, *What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods*, ACM CHI (2021).
[10] See Boush, D.M., Friestad, M., & Wright, P. (2009). Deception in the Marketplace: The Psychology of Deceptive Persuasion and Consumer Self-Protection (1st ed.). Routledge. https://doi.org/10.4324/9780203805527.
[11] For instance, inducing website visitors to disclose more personal information: John, Leslie K. et al, "Strangers on a plane: Context-dependent willingness to divulge sensitive information." Journal of Consumer Research 37, no. 5 (2011): 858-873.
[12] Now Deceptive.design, see: https://www.deceptive.design/.

that make you do things that you didn't mean to, like buying or signing up for something."[13]

The common themes across the different types of dark patterns observed by researchers can be grouped into two categories affecting how interfaces affect the choice architecture facing consumers. The first category includes interfaces that modify the set of choices available to consumers. The second category includes interfaces that manipulate the information that is available to consumers.[14] Irrespective of how they manifest in an interface, the key mechanism by which dark patterns are effective is that they take advantage of consumers' cognitive shortcuts[15] (heuristics and biases) in their decision-making processes. By doing so, dark patterns unfairly influence people's choices—the core concern of consumer protection laws. When confronted with dark patterns, consumers are manipulated, deceived, or coerced into accepting something that they would not have chosen if that were a free and informed choice.

Several enforcement actions illustrate the harms of dark patterns across the consumer journey; some of these actions feature dark patterns prior to the

---

[13] *See* What Makes a Dark Pattern... Dark? (citing studies); *see also*: Norwegian Consumer Council, *Deceived by Design*, FORBRUKER RADET 13–18 (June 27, 2018), https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf; U.K. Competition and Markets Authority. "Evidence Review of Online Choice Architecture and Consumer and Competition Harm." April 2022, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1069423/OCA_Evidence_Review_Paper_14.4.22.pdf; Acquisti, Alessandro, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon et al. "Nudges for privacy and security: Understanding and assisting users' choices online." ACM Computing Surveys (CSUR) 50, no. 3 (2017): 1-41.

[14] Ibid.

[15] Jason Collins, "We Don't Have a Hundred Biases, We Have the Wrong Model," Works in Progress, July 28, 2022, https://www.worksinprogress.co/issue/biases-the-wrong-model/.

popularization of the term. At the purchase stage of the transaction, the *Federal Trade Commission v. AMG Services, Inc*. case illustrates how the payday lender AMG Services deceived consumers by imposing undisclosed charges and inflated fees.[16] Similarly, the Commission's recent *ABCMouse* action highlights the impact of deceptive negative option marketing.[17] More recently, the New York Attorney General's Office reached a settlement with an online travel website, Fareportal, which used a number of dark patterns to trick consumers by conveying a false sense of urgency, among other techniques.[18] At the marketing stage of a transaction, the *Federal Trade Commission v. LeadClick Media* action shows how an affiliate marketing company drove traffic to the LeanSpa website by employing affiliate marketers, disguised ads, phony user testimonials, and fake news sites.[19] And in *Federal Trade Commision v. Intuit Inc.*, the Commission charged Intuit, the creators of the tax software product, TurboTax, with misleading consumers by promoting free tax-filing products that were, in fact, unavailable to millions of

[16] https://www.ftc.gov/news-events/news/press-releases/2014/06/us-district-judge-finds-payday-lender-amg-services-deceived-consumers-imposing-undisclosed-charges. 910 F.3d 417 (9th Cir. 2018), *reversed on other grounds*, 141 S. Ct. 1341 (2021), *and vacated on other grounds*, 998 F.3d 897 (9th Cir. 2021).

[17] Staff, "Children's Online Learning Program ABCmouse to Pay $10 Million to Settle FTC Charges of Illegal Marketing and Billing Practices," Federal Trade Commission, September 18, 2021, https://www.ftc.gov/news-events/news/press-releases/2020/09/childrens-online-learning-program-abcmouse-pay-10-million-settle-ftc-charges-illegal-marketing. See also the Commission's 2021 enforcement policy statement regarding negative options: https://www.ftc.gov/system/files/documents/public_statements/1598063/negative_option_policy_statement-10-22-2021-tobureau.pdf.

[18] https://freedom-to-tinker.com/2022/03/21/holding-purveyors-of-dark-patterns-for-online-travel-bookings-accountable/

[19] 838 F.3d 158 (2d. Cir. 2016); Jamie Luguri and Lior Jacob Strahilevitz. 2021. "Shining a Light on Dark Patterns," Journal of Legal Analysis. Vol. 13, pp. 43-109. https://academic.oup.com/jla/article/13/1/43/6180579

taxpayers.[20] Finally, at the sign-up stage of the consumer journey, the D.C. Attorney General's multi-state action against Google's location tracking settings illustrates how dark patterns can be used to obscure information collection and the ability of consumers to control who has access to sensitive information.[21]

We recommend that the revised Disclosure Guidelines provide businesses with additional clarity about how to communicate in a transparent and honest manner with their consumers. In particular, we offer several suggestions for where the Commission's guidance would be important.

A. Business should offer consumers symmetric choices at crucial decision-making points.

Interfaces, in general, should provide symmetry or parity among the choices offered to consumers at crucial points of decision-making. This principle strives to equalize burdens on consumer choices, moving away from disproportionally privileging options that benefit a service at the expense of the consumer, and reducing the information asymmetries and power imbalances between consumers and the services they use. For example, the process for opting out of information disclosure should not require more steps than the process for opting in.[22]

[20] Staff, "FTC Sues Intuit for Its Deceptive TurboTax 'Free' Filing Campaign," Federal Trade Commission, March 30, 2022,https://www.ftc.gov/news-events/news/press-releases /2022/03/ftc-sues-intuit-its-deceptive-turbotax-free-filing-campaign.. A parallel multi-state action was settled earlier this year. https://ag.ny.gov/turbotax-settlement-faqs
[21] Staff, "AG Racine Leads Bipartisan Coalition in Suing Google Over Deceptive Location Tracking Practices That Invade Users' Privacy," AG Racine Sues Google for Antitrust Violations Over Android App Store, July 7, 2021, https://oag.dc.gov/release/ag-racine-sues-google-antitrust-violations-over.
[22] See § 999.315(h) of the CCPA

Similarly, the process for canceling a subscription should not involve excessively greater steps than signing up. For example, when an app asks consumers whether they will consent to geolocation tracking, a choice between "Yes" and "No" is symmetrical, while in contrast, a choice between "Yes" and "Maybe later" is not. Experimental data reveals that these kinds of asymmetries are highly effective at manipulating consumers and diminishing consumer welfare.[23] Guidance on identifying asymmetric dark patterns, as well as examples of such patterns, are found in the taxonomies provided by Mathur *et. al.*[24]

Moreover, there should be a similar expectation of parity for crucial decision-making points across different modes of accessing the service so that consumers can exercise the same choices whether they are using web applications or mobile applications.[25] Indeed, as additional modes of interacting with services continue to grow – wearables, devices, smart TVs, voice assistants, mixed and/or virtual reality – there is an ongoing need to ensure the core principles of consumer protection law are respected on these new modalities. If only one modality offers a balance of opt-in/opt-out steps (for example, a desktop website version of a service) but others do not (the mobile app or IoT version of a service), this imbalance creates disproportionality that can in turn impact some consumers more than

[23] Luguri and Strahilevitz, 64-66, 75-80.
[24] Arunesh Mathur, Gunes Acar, Michael J. Friedman, Eli Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan. 2019. Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. Proc. ACM Hum.-Comput. Interact. 3, CSCW, Article 81 (November 2019), 32 pages. https://doi.org/10.1145/3359183; What Makes a Dark Pattern... Dark?
[25] Johanna Gunawan, Amogh Pradeep, David Choffnes, Woodrow Hartzog, and Christo Wilson. 2021. A Comparative Study of Dark Patterns Across Web and Mobile Modalities. Proc. ACM Hum.-Comput. Interact. 5, CSCW2, Article 377 (October 2021). https://doi.org/10.1145/3479521; Schaffner, B., Lingareddy, N., and Chetty, M. (2022) Understanding Account Deletion and Relevant Dark Patterns On Social Media. To Appear CSCW 2022.

others.[26] For example, consumers who primarily use mobile phones for their internet access can be adversely impacted by mobile applications that require access to features or policies only through a browser.

Account deletion or subscription opt-outs are particularly problematic. While registering or subscribing online is easy, services may sometimes require not only cross-modality interactions to opt-out, but also may hide opt-out mechanisms in Terms of Service, privacy policies, FAQs, or help documentation. Worse, some services may direct consumers to email, call, send a letter to, or physically visit the company to delete accounts or cancel subscriptions – despite allowing consumers to sign up digitally. For example, during the pandemic Planet Fitness required its customers to visit their local clubs in person, or to contact them by mail, in order to cancel their membership despite the clubs' pandemic-related closures.[27] Arizona Attorney General Mark Brnovich the AG filed suit against the company for these practices in May 2020.[28]

Under the proportionality/symmetry principle we recommend, services should provide opt-out mechanisms natively within an app or website, wherever consumers are able to opt-in. To facilitate this, *design consistency* may be a helpful conceptualization. Many opt-out links are embedded in website footers; in apps, these could be placed in menu footers but should be equally as easy to access. The

[26] Ibid.
[27] Planet Fitness. Frequently Asked Questions. https://www.planetfitness.com/about-planet-fitness/customer-service.
[28] "Planet Fitness Sued Over Billing Practices During Pandemic - NHPR." 15 May. 2020, https://www.nhpr.org/nh-news/2020-05-15/planet-fitness-sued-over-billing-practices-during-pandemic.

2013 Disclosure Guidance[29] notes that advertisers should consider screen-size dynamics and differences between touch or mouse-click modalities; we suggest that advertisers should be encouraged to consider where consumers might *expect* to access opt-outs and other relevant settings within an app or website and place them (and, where relevant, disclosures) there.[30] We suggest further that the Commission provide guidance on managing opt-out proportionality across different offerings of the same service. Relatedly, we suggest the Commission extend its guidance to cover additional input modalities beyond touchscreens, mice, and keyboards, such as voice assistants.[31] [32]

B. Businesses should not preselect choices (defaults) that favor the interest of the provider at the expense of the consumer.

Interfaces should not use what are referred to in the literature as "bad defaults," which preselect choices that favor the interest of the service provider at

[29] Federal Trade Commission of the United States. ".com Disclosures: How to Make Effective Disclosures in Digital Advertising." 2013. https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf

[30] Habib, Hana, Sarah Pearman, Jiamin Wang, Yixin Zou, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. "" It's a scavenger hunt": Usability of Websites' Opt-Out and Data Deletion Choices." In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, pp. 1-12. 2020.

[31] Kentrell Owens, Johanna Gunawan, David Choffnes, Pardis Emami-Naeini, Tadayoshi Kohno, and Franziska Roesner. "Exploring Deceptive Design Patterns in Voice Interfaces." European Symposium on Usable Security (EuroUSEC), September 2022.

[32] Major, David, Danny Yuxing Huang, Marshini Chetty, and Nick Feamster. "Alexa, who am I speaking to?: Understanding users' ability to identify third-party apps on amazon Alexa." ACM Transactions on Internet Technology (TOIT) 22, no. 1 (2021): 1-22.

the expense of consumers.[33] Bad defaults share traits with the *roach motel*[34] and *preselection*[35] dark patterns, trapping consumers into disadvantageous, difficult-to-escape situations, and making choices for consumers without prompting. Several issues arise with bad default settings: first, controls for these options might not be provided (thus, disclosed) during new user interactions (like account registration). This denies consumers the ability to make optional selections up front and draws on themes from the *hidden information* class of dark patterns. Second, whether or not these controls are provided to consumers early on, the bad default choices are selected for the service's interests. This is unfair to consumers whenever the service's best interests and the consumer's do not align, and is additionally an issue of proximity and placement. Third, these settings may be offered in high levels of granularity without bulk-action toggles (Accept All/Reject All), which forces consumers to individually un-check each setting in order to turn them off.

[33] Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. 2016. Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. Proceedings on Privacy Enhancing Technologies. Volume 4. Pages 237–254. https://petsymposium.org/2016/files/papers/Tales_from_the_Dark_Side__Privacy_Dark_Strategies_and_Privacy_Dark_Patterns.pdf. See also, generally: This website uses nudging: MTurk workers' behaviour on cookie consent notices. Proceedings of the ACM on Human-Computer Interaction, 5(CSCW2), Oct 2021; Midas Nouwens et al. Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. ACM, April 2020; Christine Utz et al. (Un)informed consent: Studying GDPR consent notices in the field. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS '19, pages 973–990, 2019; Stutzman, Frederic D., Ralph Gross, and Alessandro Acquisti. "Silent listeners: The evolution of privacy and disclosure on Facebook." Journal of privacy and confidentiality 4, no. 2 (2013): 2.

[34] Harry Brignull. "Types of Deceptive Design." https://www.deceptive.design/types

[35] Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L. Toombs. 2018. The Dark (Patterns) Side of UX Design. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18). Association for Computing Machinery, New York, NY, USA, Paper 534, 1–14. https://doi.org/10.1145/3173574.3174108

C. Businesses should disclose material information in a manner that allows consumers to make informed decisions.

More generally, the Commission should ask businesses to use designs that present material information to consumers in a manner reasonably likely to allow users to make informed choices. For example, online services should fully disclose all costs related to a product or service upfront and not engage in "drip pricing" where the full cost is disclosed only upon payment,[36] or hidden fees are tacked on to the price paid at check-out without disclosure or explanation.[37] The Commission could also consider a heightened requirement to present information in a manner that serves the best interest of the consumer at critical decision points in the customer flow.

D. Businesses should be encouraged to follow ethical design principles.

The Commission should encourage businesses to follow ethical design principles when designing their interfaces. When designing ads, for example, this includes making ads distinguishable from user-generated content on social

[36] See generally: https://www.ftc.gov/news-events/events/2012/05/economics-drip-pricing; https://www.washingtonpost.com/business/drip-pricing-is-turning-checkout-into-a-nasty-surprise/2022/06/16/798da2ee-ed68-11ec-9f90-79df1fb28296_story.html

[37] See generally: Tom Blake et al., Price salience and product choice. Marketing Science, 40:619–636, 2021; Markus Dertwinkel-Kalt et al., To buy or not to buy? Price salience in an online shopping field experiment. European Economic Review, 130, 2020.

platforms, or from content articles on news websites, to avoid misleading consumers. For example, across many platforms today, links used to label sponsored content (e.g., "sponsored," "ad," or "promoted" labels), product recommendations, private labels, and native advertisements do not meet the FTC's clear and conspicuous standard, and instead are visually minimized and difficult for consumers to locate and observe.[38] Similarly, the Commission should prohibit interfaces that inject a misleading sense of urgency or scarcity (for example, using provably false countdown timers or false 'limited time offers') to manipulate a consumer into taking an action. The Commission should also address the use of interfaces that interrupt consumers to display ads or promote paid features.[39]

At a higher level, ethical design practices should take into account how different demographics, especially vulnerable populations, may interact with an interface. All online service providers should consider vulnerable populations in their design practices, and create interfaces and disclosures that do not take advantage of consumers' vulnerabilities. For example, variables such as education level can influence a consumer's ability to discern a dark pattern.[40] The

[38] Amazeen, Michelle A, and Bartosz W Wojdynski. "The Effects of Disclosure Format on Native Advertising Recognition and Audience Perceptions of Legacy and Online News Publishers." Journalism 21, no. 12 (December 2020): 1965–84. https://doi.org/10.1177/1464884918754829; Brashier, Nadia M., and Daniel L. Schacter. "Aging in an Era of Fake News." Current Directions in Psychological Science 29, no. 3 (June 2020): 316–23. https://doi.org/10.1177/0963721420915872.
[39] Linda Di Geronimo, Larissa Braz, Enrico Fregnan, Fabio Palomba, and Alberto Bacchelli. 2020. UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception. Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376600.
[40] See generally: Luguri and Strahilevitz, 80-81; Chen, Janet X., Allison McDonald, Yixin Zou, Emily Tseng, Kevin A. Roundy, Acar Tamersoy, Florian Schaub, Thomas Ristenpart, and Nicola Dell. "Trauma-Informed Computing: Towards Safer Technology Experiences for All." In CHI Conference on Human Factors in Computing Systems, pp. 1-20. 2022.

Commission can recommend that companies test the usability and comprehensibility of interfaces across the different demographics that use the services in order to incorporate design changes which reflect varying consumer needs.

Similar to existing FTC guidance adopting a privacy by design framework, we ask that the Commission consider requiring "consumer-centered" design at digital decision points that have high stakes or direct economic or information disclosure consequences for consumers, such as financial transactions or consent architectures.[41] Our suggestion is based on the premise that consumers should be able to transact and make decisions, particularly decisions with direct financial consequences, free from distraction or undue influence. By consumer-centered design, we mean visual design that does not incorporate deceptive, coercive, or manipulative design elements, but instead is based on generally accepted design principles (validated through academic research or by practitioner design communities) to facilitate decision-making or completing an action (such as making a purchase) in a manner that supports informed and fair decision-making.

A consumer-centered design should, as a matter of principle, be both impartial and not cause harm; promote fairness by creating at minimum an equitable balance of power between actors; and, be composed in such a way that it facilitates interaction and mutual goals rather than favoring or coercing one actor

[41] "Neutral" design is another term used to describe this concept, which is emergent. Professor Woodrow Hartzog also suggests "impartial design," "honest design," or "loyalty design." See generally: Hartzog, Privacy's Blueprint; and, Richards, Neil M. and Hartzog, Woodrow, A Duty of Loyalty for Privacy Law (July 3, 2020). 99 Washington University Law Review 961 (2021).

in achieving their goal at the expense of the other. We suggest that consumer-centeredness is achievable through ethical, non-harmful design that facilitates rather than manipulates consumer interaction.

E. Businesses should disclose how they use personal data to shape the online choice architecture.

Finally, we draw the Commission's attention to an emergent form of dark patterns that are data-driven and dynamic (e.g., personalized to the individual consumer and more generally adaptive).[42] Such adaptive dark patterns include manipulative choice architectures that adapt to a user by modifying the design of an interface to respond to individual consumer behaviors and attributes, or by directly attempting to modify a consumer's behavior over time.

While these types of adaptive dark patterns have not been widely observed at scale as of yet, other consumer protection regulators have noted the concerns about such practices and the importance of keeping a watch on their development. For instance, the UK CMA's report on algorithms notes that the ranking and positioning of search results, scarcity messages generated by algorithms, and "decisions related to bundling of products or services for targeted sales" are examples of algorithmically generated manipulation. The report calls for further research on the subject.[43]

[42] Lauren E. Willis. Deception By Design. 34 Harvard Journal of Law & Technology 115 (2020).
[43] UK Competition & Markets Authority. "Algorithms: How they can reduce competition and harm consumers." January 19, 2021. Available at:

As an initial step, we recommend the Commission monitor the way companies use data, including personal data, to adapt the appearance of choice architectures. If key decision points, such as check outs or consent flows in the consumer's journey are being targeted for customization or personalization, we suggest the Commission provide guidance to companies to disclose that action to consumers.

2. The Commission should examine how consumer protection authorities across different countries are addressing dark patterns in developing its guidance. (Question 1)

Various jurisdictions around the world are working to address the problem of proliferating dark patterns online. We summarize some of the key initiatives here. While each jurisdiction operates in its unique context, the main takeaways from this brief survey are twofold. *First*, dark patterns are a set of practices that are being studied extensively because of the harm they are causing consumers.[44] *Second*, there are strategies to counteract these harms that are worth drawing lessons from as the FTC develops its own guidance.

A. European Union

The new Digital Services Act (DSA) imposes restrictions on providers of intermediary services who use their online interface (either through structure,

---

https://www.gov.uk/government/publications/algorithms-how-they-can-reduce-competition-and-harm-consumers.

[44] Jennifer King and Eli MacKinnon. "Do the DSA and DMA Have What It Takes To Take on Dark Patterns?" Tech Policy Press, June 23, 2022. https://techpolicy.press/do-the-dsa-and-dma-have-what-it-takes-to-take-on-dark-patterns/

design or functionality), to impair consumers' ability to make free, autonomous and informed decisions or choices (Article 13a).[45] DSA Recitals state that recipients of services should be empowered to make decisions about matters such as acceptance and changes to terms and conditions, advertising practices, privacy and other settings and recommender systems without being subjected to practices which exploit cognitive biases, prompting consumers to purchase goods or services they do not want or to reveal personal information they would prefer not to (Recital 39a). The DSA provides specific examples of prohibited practices such as:

1. giving unequal visual prominence to any consent options when asking the consumer for a decision;
2. repetitively requesting or urging the receipting to make a decision such as repeatedly requesting consents to data processing where consent has previously been refused (especially in the form of a pop-up that interferes with the user experience) or has been refused through the use of automatic refusal configurations;
3. urging a consumer to change a setting or configuration after the consumer has already made a choice; or
4. making the procedure to cancel a service significantly more cumbersome than signing up to it.

B. China

[45] "The new EU Dark Pattern laws: changes to the Digital Services Act." 28 Jan. 2022, https://www.lexology.com/library/detail.aspx?g=4340915c-b302-4d73-b042-7cfff85c12f1.

The Chinese government is tackling problems with dark patterns through regulation. In November 2021, the State Administration for Market Regulation released the Measures for the Administration of Internet Advertising ("Draft Regulations") that contains various proposals to regulate the use of dark patterns.[46] For example, they have proposed a requirement that there should be a one-click closing button for pop-up advertisements, start-up playback, video insertions, and other such interstitial advertising. The Draft Regulations also require companies to collect and maintain data about their algorithmic recommendations for personalized advertising to allow the government to evaluate if those algorithms might be manipulating users.[47]

C. Australia

In September 2021, the ACCC (Australian Competition & Consumer Commission) released its third digital platform services inquiry report that outlined potential measures that search engines and browsers could adopt to mitigate the use of dark patterns.[48] The report also recommended prohibiting "conduct that is particularly harmful to consumers, and significantly impedes consumer choice."[49] As it relates to the use of dark patterns to undermine meaningful consent, in a separate discussion paper, the ACCC discussed how

[46] "互联网广告管理办法."https://www.samr.gov.cn/hd/zjdc/202111/P020211126528180635858.pdf.
[47] Ibid.
[48] "The new EU Dark Pattern laws: changes to the Digital Services Act." 28 Jan. 2022, https://www.lexology.com/library/detail.aspx?g=4340915c-b302-4d73-b042-7cfff85c12f1.
[49] Ibid.

including more stringent criteria for what constitutes consent, might also limit the ability for companies to use dark patterns.[50]

D. United Kingdom

In the United Kingdom, the regulators are focused on researching the impact of dark patterns and online choice architecture more generally. The Competition and Markets Authority (CMA) recently published two papers in April 2022 discussing and summarizing evidence on online choice architecture and how it potentially causes harm to consumers.[51] The CMA's research describes how those who design—the user experience and interaction designers, the content designers and the marketers—can be thought about as choice architects, and the design of the environment they create is the choice architecture. Common examples of choice architecture include the order of products in search results, the number of steps needed to cancel a subscription, or whether an option is selected by default. The CMA cites a growing body of research that suggests that such elements affect consumers and markets in significant ways.[52] The CMA notes that its choice to use the term "choice architecture" is deliberately neutral to account for the differences in how online experiences are structured. For example, it explains, well-designed

[50] Ibid.
[51] U.K. Competition and Markets Authority. "Online Choice Architecture: how digital design can harm competition and consumers." April 2022, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1066524/Online_choice_architecture_discussion_paper.pdf. See also: U.K. Competition and Markets Authority. "Evidence Review of Online Choice Architecture and Consumer and Competition Harm." April 2022, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1069423/OCA_Evidence_Review_Paper_14.4.22.pdf.
[52] Ibid.

websites, apps or digital services built with consumers' interests in mind will help consumers choose between suitable products, make transactions faster, and recommend new relevant products or services. However, choice architectures can also hide crucial information, set default choices that may not align with consumer preferences, or exploit consumers by drawing attention to scarce products.

The CMA notes that while the improper influence of consumers has always been a subject of regulatory concern, the speed and scale of data collection, experimentation, and targeted personalization available to businesses online also facilitates the development and optimization of choice architecture in real time.[53] As a result, the CMA has a multi-prong strategy to tackle abuses. First, it will challenge choice architectures that mislead and harm consumers or undermine their trust and confidence in online markets. Second, it will use a combination of behavioral science, data science, and other methods to determine the prevalence of harmful practices. Third, it will engage in bilateral and multilateral engagement with other authorities and regulators to develop effective strategies to regulate harmful conduct. Fourth, it will raise consumer and business awareness of such practices.

[53] U.K. Competition and Markets Authority. "Online Choice Architecture: how digital design can harm competition and consumers." April 2022, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1066524/Online_choice_architecture_discussion_paper.pdf.

3. The Commission should consider research that documents the limited effectiveness of boilerplate online disclosures to cure consumer confusion. (Questions 3 & 4)

A number of studies have shown that legalistic, long form disclosures are not read or understood by the average consumer. The legion of problems with notice and consent mechanisms that rely on online disclosures have been well documented in the behavioral literature.[54] In other words, the Commission should be wary of requiring additional disclosures to become the cure for unfair or deceptive online practices. There are studies that demonstrate that disclosures shown close to the time of the decision and relevant to that decision are a lot more effective in educating consumers about their choices. Acquisti and others argue in "Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online," certain forms of privacy nudges may have a greater impact based on when they are seen.[55] As Egelman and others found in "Timing Is Everything?: The Effects of Timing and Placement of Online Privacy Indicators," participants in a study who viewed privacy indicators before visiting a website were more greatly impacted than those who saw the indicators once the users already arrived at the

[54] Reviews of relevant empirical work can be found in Acquisti, Alessandro, Laura Brandimarte, and George Loewenstein, "Privacy and human behavior in the age of information," Science 347, no. 6221 (2015): 509-514 and in Acquisti, Alessandro, Laura Brandimarte, and George Loewenstein, "Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age," Journal of Consumer Psychology 30, no. 4 (2020): 736-758; Florian Schaub, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor. 2015. A design space for effective privacy notices. In Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security (SOUPS '15). USENIX Association, USA, 1–17.

[55] Alessandro Acquisti *et al.*, "Nudges for Privacy and Security," ACM Computing Surveys 50, no. 3 (2018): pp. 1-41, https://doi.org/10.1145/3054926, 44.

website.[56] As a way forward, we recommend that consumer-centered disclosures should be (1) relevant to the context of transaction, (2) understandable by the respective consumer audience/segment, and (3) actionable, in that the disclosure needs to be associated with the ability to express an informed decision/choice.[57]

4. The Disclosure Guidelines for mobile interfaces should be updated to curb problematic practices in mobile apps. (Questions 10 & 11)

The 2013 Disclosure Guidelines briefly discuss mobile interfaces and provide some guidance to account for differences in how information is conveyed on handheld devices. This includes mobile optimization, screen size, scrolling differences, touch/click differences, and technological limitations (e.g., disclosures using Flash). But the guidance mostly pertains to differences between advertising on desktop devices versus handheld devices. Since that time, mobile apps have evolved considerably. For example, Google Play was responsible for 111.3 billion downloads in 2021 and iOS had 32.3 billion downloads. As mobile apps have become increasingly ubiquitous, the design of mobile applications have also evolved, creating the opportunity for the proliferation of mobile dark patterns. A new study of 1,759 iOS apps before and after Apple implemented a major privacy feature last year (App Tracking Transparency (ATT)) found the permission made tracking more difficult by preventing the collection of the Identifier for Advertisers

[56] Serge Egelman *et al.*, "Timing Is Everything?: The Effects of Timing and Placement of Online Privacy Indicators," Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, April 2009, https://doi.org/10.1145/1518701.1518752.
[57] Schaub & Cranor, 2020. Usable and Useful Privacy Interfaces. in An Introduction to Privacy for Technology Professionals. IAPA.

(IDFA), which can be used for cross-app user tracking. Additionally, researchers found evidence of app makers engaging in the privacy-hostile fingerprinting of consumers, through the use of server-side code, in a bid to circumvent Apple's ATT — suggesting that developers may attempt to find other ways to keep tracking iOS users.[58]

The revised guidelines should address the tactics mobile app developers commonly use to exploit consumers. While it is clear that mobile design has different needs than browser design, this should not preclude developers from making relevant information clear to consumers, nor from fairly presenting all relevant options possible to them.

As we noted previously, the revised Disclosure Guidelines should require symmetrical choices at crucial decision points for consumers no matter the type of device or app they use to interact with content. DiGeronimo *et al.*[59] in a survey and experiment on dark patterns in mobile apps, observed that mobile apps frequently interrupted consumers to display ads or promote paid features. In particular, they note how on mobile apps, pop-up ads can take up the entire viewable mobile screen space, and make it difficult for a consumer to close the ad.[60] App developers can also manipulate the environment to affect the interactivity of an ad (*e.g.,*

[58] "Study of Apple's ATT impact highlights competition concerns." 8 Apr. 2022, https://techcrunch.com/2022/04/08/apple-att-impact-study/.
[59] Linda Di Geronimo, Larissa Braz, Enrico Fregnan, Fabio Palomba, and Alberto Bacchelli. 2020. UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception. Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376600.
[60] Ibid.

interactive games[61] or scrolling features in ads), as well as the placement of disclosures within the ad itself. iOS and Android platforms, moreover, allow for ads that require consumers to play a game or wait before skip buttons appear.[62] Given the aim of promoting choice symmetry, consumers should instead see material disclosures in the same environment that they view an advertisement. In other words, a mobile app consumer should not be forced to exit the app and open a desktop site to view disclosures that are meant to be provided in a "clear and conspicuous" manner.[63] The revised guidance should address these types of dark patterns directly, especially for pop-ups or other disruptive designs. The guidance should require app developers to present clear and conspicuous disclosures on the first screen that consumers visit when opening ads (mobile websites, even dynamically designed ones, may require consumers to scroll to see disclosures).

5. The Commission should clarify that hyperlinks should not be used to obscure material information. (Question 8)

The primary function of a hyperlink is to signal the existence of information not contained on the existing screen or page through its presence on a digital screen or within the consumer interface of an application. But when using hyperlinks, it is critical to look beyond their label, visual appearance, and where they are located in the disclosure and examine whether the information contained

[61] Ibid.
[62] Mariana Vargas, "Dark Design Patterns in Your Everyday Apps," Medium (UX Planet, July 22, 2021), https://uxplanet.org/dark-design-patterns-in-your-everyday-apps-3627e439a8a1.
[63] Johanna Gunawan, Amogh Pradeep, David Choffnes, Woodrow Hartzog, and Christo Wilson. 2021. A Comparative Study of Dark Patterns Across Web and Mobile Modalities. Proc. ACM Hum.-Comput. Interact. 5, CSCW2, Article 377 (October 2021). https://doi.org/10.1145/3479521

in the linked document is material to the transaction. If the information is material, then it should be made an unavoidable part of the transaction flow.[64] For instance, in the FTC's *ABCMouse* action, the hyperlink to the subscription information within the service's "Terms & Conditions" was not sufficient to cure the deception that caused consumers to enroll in renewable services. We recommend the 2013 Disclosure Guidelines guidance addressing hyperlink text, color, and placement be clarified to state that hyperlinks should not obscure essential information to consumers. If all relevant options must be made visible to consumers, then hyperlinks cannot be employed to obscure the information necessary for decision-making. At the same time, overloading consumers with extraneous information, such as requiring that consumers page through an entire terms of service document that contains the material information but does not call it out or highlight it for them, is not a solution.

Research has shown that obscure hyperlinks can also present serious security risks. While phishing attacks have introduced significant well-known risks in the past, more recent research has also demonstrated that hyperlinks can be a vector for attack in smart homes, even allowing remote attackers to control devices in the consumer's home without the consumer's consent or awareness—*even when the original link itself is legitimate*.[65] Given these risks, hiding information behind obscure hyperlinks not only introduces friction into the information flow, but also introduces additional (unnecessary) vectors for potential attack.

[64] Jennifer King and Adriana Stephan. Regulating Dark Patterns in Practice – Applying the California Privacy Rights Act. Georgetown Technology and Law Review. 5 Geo. L. Tech. Rev. 251 (2021).
[65] Acar et al., 2018

6. The Disclosure Guidelines should anticipate issues that may arise with respect to advertising that appears in mixed and/or virtual reality, or the metaverse, by providing clarity that services should interact with consumers in those new mediums in a fair and transparent manner. (Question 14)

While the development of mixed reality (MR), virtual reality (VR), and/or "metaverse" modes of interacting with services is still in their infancy, companies have made significant investments in this space, and the Commission should clarify that these services should interact with consumers in those new mediums in a fair and transparent manner. Compared to mobile and web mediums, ads in MR/VR have the potential to be especially harmful. The immersive nature of the medium can present health and safety concerns for consumers[66] (so called 'shockvertising'). Additionally, because mixed or virtual reality involves consumers interacting with services in an unfamiliar medium, consumers will need additional information about what distinguishes an ad from virtual reality, what potential harms may occur, and how different entities in MR/VR spaces collect data.[67] As examples of VR/AR ads begin to emerge, we recommend that the Commission consider the unique and exacerbated harms that can arise from these types of ads. For example, researchers have identified how it is harder for users to avoid ads in more immersive environments.[68] In sum, we ask that choice parity and symmetry

[66] For general discussions about risks from malicious virtual content in MR/VR, see: https://ar-sec.cs.washington.edu/files/lebeck-arsec-hotmobile19.pdf; https://ar-sec.cs.washington.edu/files/arsec-hotmobile16.pdf; https://arxiv.org/abs/1806.10557.
[67] Abraham Mhaidli and Florian Schaub. "Identifying Manipulative Advertising Techniques in XR Through Scenario Construction." CHI Conference on Human Factors in Computing Systems, May 2021.
[68] Ibid.

principles we identified earlier should be a core value of the design of VR/AR ads. Finally, we recommend that the Commission be watchful for emergent forms of dark patterns that may take hold in this space.

* * *

In closing, we appreciate the opportunity to provide these comments and welcome the opportunity to discuss any questions that may arise.

Respectfully submitted,

Alessandro Acquisti
Trustees Professor of Information Technology, Heinz College, Carnegie Mellon University

Caitlin Burke*
PhD Candidate, Department of Communication, Stanford University

Marshini Chetty
Assistant Professor, Department of Computer Science, University of Chicago

David Choffnes
Associate Professor, Khoury College of Computer Sciences, Northeastern University

Serge Egelman
Research Director, Usable Security and Privacy Group, International Computer Science Institute (ICSI)

Colin M. Gray
Associate Professor of Computer Graphics Technology, Purdue University

Johanna Gunawan*
PhD Candidate, Khoury College of Computer Sciences, Northeastern University

Woodrow Hartzog
Professor of Law, Boston University School of Law

Jane Im
PhD Candidate, School of Information & Division of Computer Science and Engineering, University of Michigan

Jennifer King*
Privacy and Data Policy Fellow, Stanford Institute for Human-Centered Artificial Intelligence

Mihir Kshirsagar*
Clinic Lead, Princeton's Center for Information Technology Policy

Jonathan Mayer
Assistant Professor of Computer Science and Public Affairs, Princeton University

Abraham Mhaidli*
PhD Candidate, School of Information, University of Michigan

Arvind Narayanan
Professor of Computer Science, Princeton University

Franziska Roesner
Associate Professor, Paul G. Allen School of Computer Science & Engineering, University of Washington

Brennan Schaffner
PhD Student, Department of Computer Science, University of Chicago

Florian Schaub
Assistant Professor, School of Information, University of Michigan

Lior Strahilevitz
Sidley Austin Professor of Law, University of Chicago

Nicole Tong

Research Assistant, Stanford Institute for Human-Centered Artificial Intelligence

Charlie Wang*
Summer Intern, Princeton's Center for Information Technology Policy

Christo Wilson
Associate Professor, Khoury College of Computer Sciences, Northeastern University

Eric Zeng*
Postdoctoral Researcher, CyLab, Carnegie Mellon University

* denotes signatories who provided substantial drafting assistance

Contact: 609-258-5306; mihir@princeton.edu