***

The Rebound Effect
Remarks from Chief Technologist Stephanie T. Nguyen
As Prepared for Delivery: National Press Club, Washington D.C.
The U.S. Artificial Intelligence & Sustainability Summit

June 2024

***

Thank you for inviting me to speak at the US Artificial Intelligence & Sustainability Summit. My name is Stephanie Nguyen, I'm Chief Technologist at the Federal Trade Commission - I'm head of the Office of Technology and today's remarks are my own views and not that of the Commission or any Commissioner.

I'm honored to be here to get to meet people like Dr. Dorsey, an accomplished and respected fish biologist. I was struck by the similarities of the work we do in our roles: how we navigate quickly changing landscapes, how we establish resiliency to protect people, how we translate research into action.

The theme of this Summit as it was shared with me is to "promote sustainability and economic prosperity." I'd like to do this by focusing on how the Federal Trade Commission (FTC) defends and protects these values by enforcing the law in two core areas: protecting consumers and competition.

There's a million ways to exploit consumer vulnerabilities. Today I'd like to talk about deceptive design patterns.

Deceptive patterns go by many names. In my remarks I'll use "dark patterns" moving forward for clarity. These can be defined as design tricks that manipulate consumers into taking unwanted actions.[1]

There's an extensive taxonomy, or dictionary of dark pattern terms to capture the various ways corporations trick, trap or coerce people.

Here are some reflex thoughts that may have just come to mind:

- Users can avoid dark patterns if they know about them.
- Notice and choice is an effective solution
- Dark patterns only have short term, innocuous effects.

Today, I'd like to redirect these thoughts and provide an alternative way to conceptualize dark patterns that represents the realities of commerce in 2024.

I will first discuss how the growth of dark patterns researchers and investigators is part of a symphonic response due to the years of failed privacy protections of notice and choice — a failure that has been

[1] https://www.deceptive.design/

thoroughly noted by leadership at the FTC.[2] Second, I will outline how dark pattern elements mirror a broader core business model. The way law enforcers approach such harms must be adapted with rapidly evolving technologies. Finally, I will expand on these vulnerabilities and highlight how they can be manifested through three categories of harms: daily indignities, systemic disadvantages and information asymmetries.

Section 1: A Rebound from the Failures of Notice & Choice Models

I'd like to set context by describing an era I call the rebound from the failures of notice and choice models. I've designed thousands of user interface elements and wireframes that have been deployed in products to millions of people.

Design practitioners can use pattern libraries and style guides — a reusable collection of design elements and layouts that have been tried and true with other websites, apps, and platforms. Nearly every product I've worked on required some version of onboarding and disclosing a mountain of legalese.

To get people's "consent," through a digital interface, developers and designers must give "notice" which often comes in the form of one of these go-to design patterns: a fleeting tiny pop-up window that jams in privacy policy text with a checkbox, or a button that says, "I agree."

In practice, it is widely known that notice and choice is ineffective,[3] confusing,[4] and gives the illusion of choice and empowerment.[5] Recall the 2010s era where the "Internet of Things," smartwatches, and heads-up displays entered the marketplace. The failures of notice and choice exacerbated as screens got tinier or at times just did not exist. Technology changed swiftly over the years, but the "privacy protecting" mechanism of notice and choice didn't.

Around the same time, dark patterns research began to take shape amid the growth of digital platforms, the desire to collect of vast amounts of user data,[6] and the field of behavioral science and nudges took shape,[7] starting with the coining of "dark patterns" in 2010.[8] And since then, the field has continued to

---

[2] https://www.ftc.gov/system/files/ftc_gov/pdf/20240417-Reidenberg-Lecture-final-for-publication-Remarks-Sam-Levine.pdf

https://www.ftc.gov/system/files/ftc_gov/pdf/remarks-of-samuel-levine-at-nad-2023.pdf

https://www.ftc.gov/system/files/ftc_gov/pdf/testimony-chair-khan.pdf

https://www.ftc.gov/system/files/documents/public_statements/1597790/20211021_isp_privacy_6b_statement_of_chair_khan_final.pdf

[3] https://www.sciencedirect.com/science/article/abs/pii/S1094996804701085

[4] https://www.researchgate.net/publication/255588023_A_Longitudinal_Assessment_of_Online_Privacy_Notice_Readability?__cf_chl_tk=.qHaB.pmoDwRQGlxbxYjfdN9B42WSeKo2de3k_lE5xQ-1718079995-0.0.1.1-4884

[5] https://www.ftc.gov/sites/default/files/documents/public_comments/privacy-roundtables-comment-project-no.p095416-544506-00057/544506-00057.pdf

[6] https://www.nytimes.com/2023/05/03/opinion/ai-lina-khan-ftc-technology.html

[7] https://www.hannahsellam.com/blog/dark-patterns-interview-of-harry-brignull-the-inventor-of-this-concept

[8] https://www.vox.com/recode/22351108/dark-patterns-ui-web-design-privacy

flourish. Scholars, researchers, investigators, and practitioners have dutifully expanded the field, provided more definitions, more taxonomies, and more vernacular to engage on the topic. It empowered a movement of investigators: the vigilantes for unscrupulous business activity. [9] [10] [11] [12] [13] [14] [15] [16] [17] [18] [19] [20]

With generative AI, "data is the new oil," as FTC Staff outlined in a recent publication.[21] Corporations can use their outsized power and information asymmetries to extract massive amounts of personal information[22] as they go about their daily lives. This includes scooping up: a person's location,[23] purchase or browsing history,[24] and fertility[25] and health information[26] [27] [28] [29] in exchange for signing up for a new platform or service.

---

[9] https://doi.org/10.1145/3173574.3174108
[10] https://arxiv.org/pdf/2101.04843
[11] https://johannagunawan.com/assets/pdf/gunawan-2021-cscw.pdf
[12] https://doi.org/10.1145/3313831.3376600
[13] https://johannagunawan.com/assets/pdf/gunawan-2023-chiworkshop.pdf
[14] https://doi.org/10.1145/3313831.3376321
[15] https://darkpatternstipline.org/
[16] https://doi.org/10.1145/3368860.3368865
[17] https://doi.org/10.1016/j.copsyc.2019.08.025
[18] https://doi.org/10.1515/popets-2016-0038
[19] https://johannagunawan.com/assets/pdf/gunawan-2021-chiworkshop.pdf
[20] https://doi.org/10.1145/3313831.3376600
https://doi.org/10.1145/3359183
https://doi.org/10.1145/3274388
https://chi2024.darkpatternsresearchandimpact.com/
[21] https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/02/ai-other-companies-quietly-changing-your-terms-service-could-be-unfair-or-deceptive
[22] https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security#footnote-4-p51273
[23] https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-will-ban-inmarket-selling-precise-consumer-location-data

[24] https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf
[25] https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google

https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc

[26] https://www.ftc.gov/news-events/news/press-releases/2024/04/alcohol-addiction-treatment-firm-will-be-banned-disclosing-health-data-advertising-settle-ftc
[27] https://www.ftc.gov/news-events/news/press-releases/2024/04/proposed-ftc-order-will-prohibit-telehealth-firm-cerebral-using-or-disclosing-sensitive-data
[28] https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising
[29] https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-gives-final-approval-order-banning-betterhelp-sharing-sensitive-health-data-advertising

"Let's not mince words," Bureau of Consumer Protection Director, Samuel A.A. Levine said in recent remarks. "Notice and choice is a fantasy world, divorced from the reality of how people live or how firms operate."[30]

Section 2: The Backdrop of Generative AI & Core Business Incentives

Note that these manipulative practices existed since the dawn of commerce. Centuries ago, chatbots or modern digital interfaces did not exist. But there were manipulative tactics like false ads, opaque pricing, limited choices, and coercive selling tactics. And in its 100+ year history, the FTC has brought a plethora of cases and engaged on this topic, including a recent report on dark patterns led by the brilliant staff in the Bureau of Consumer Protection.[31]

Today, the scale and velocity of technological advancements including generative AI means data is a critical input required to power large language models. Over time, companies can better control interfaces to optimize for more data or more profits. Some factors that highlight how generative AI can impact the reach, spread, and impact of dark patterns include:

- **Scale and speed to reach more people at a faster rate.** Companies can experiment with new design features in digital environments than they can in physical, brick-and-mortar ones.
- **Quick iteration and deployment.** Companies can test, refine, and adapt patterns more quickly through behavioral analysis such as A/B testing and learning algorithms.
- **The ability to hyper-target content.** Companies can gather massive amounts of data on individual demographics, purchases, behaviors to better target individuals via content, images, code, and platforms.
- **Barriers of choice due to concentration of power.** When a few large firms control vast ecosystems of infrastructure, cloud computing, data and models - this can restrict options and stifle innovation.

A dark pattern can often be visually observed at the front-end layer of a product or service. However, designs are inextricable from the business model incentives. Beyond just looking at the surface, we must ask - what led to this? What factors led to the decisions to design user interfaces that can lead to more data collection or more profits?

"The FTC is taking bold steps to move away from the flawed 'notice and choice' privacy framework and establish substantive protections for consumers' personal data," said Chair Khan.[32]

Section 3: Consumer Vulnerabilities are Exploited in Three Ways: Daily Indignities, Systemic Disadvantages and Information Asymmetries

Dark patterns and more broadly, product design and implementation decisions made by companies can exploit consumer vulnerabilities. These vulnerabilities can be exploited through three core ways: daily indignities, systemic disadvantages and information asymmetries - which I outline below and illustrate with FTC cases.

---

[30] https://www.ftc.gov/system/files/ftc_gov/pdf/20240417-Reidenberg-Lecture-final-for-publication-Remarks-Sam-Levine.pdf

[31] https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf

[32] https://www.ftc.gov/system/files/ftc_gov/pdf/testimony-chair-khan.pdf

The first category of exploitation relates to designs that facilitate daily indignities, or death by a thousand cuts. FTC actions in several cases have highlighted forms of daily manipulation that can and have inflicted harm on millions of users.

> The agency took action against Amazon for allegedly duping millions of consumers in enrolling in Prime "without consent and sabotaging their attempts to cancel."[33] Design is inseparable from its business model. Even when Amazon and its leadership were aware - the Commission's complaint alleges that they "slowed, avoided, and even undid UX changes that would reduce [enrollment] because those changes would also negative affect Amazon's bottom line."[34]
>
> Daily harms can come as continuous offenses - or series of user interaction elements in a product. In a complaint against Publishers Clearing House (PCH), the FTC alleged the company misled consumers to believe that "a purchase [was] necessary . . . and would increase their chances of winning," added surprise shipping fees, and misrepresented its policies on selling users' personal data to third parties.[35] The stipulated order mandated significant design and information architecture revisions and required PCH to destroy ill-gotten data and preserve records of any behavioral or psychological research or usability testing to help prevent further use of dark patterns.
>
> In Credit Karma,[36] the FTC alleged the company's website and mobile app tricked consumers with false "pre-approved" credit offers and wasted "significant time and harm[ed] their ability to secure other financial products in the future."

The second category of vulnerabilities relates to product design decisions that lead to systemic disadvantages. This includes default product choices that may lead a user to making decisions they would not have otherwise done.

> The FTC's complaint[37] against Fortnite maker Epic Games alleged that their on-by-default voice chat system allowed strangers to communicate with children and teens, resulting in threats, bullying and sexual harassment.[38] The FTC settlement requires Epic to change its default settings.[39]
>
> Defaults are indeed powerful and the FTC has acted to ensure the burden is not on the user to opt-out or upgrade their software. For example, in its complaint against peer-to-peer file-sharing app developer, Frostwire LLC, the Commission alleged that the company used default features to expose sensitive personal files within their file-sharing network.[40] The stipulated order resolving

---

[33] https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-takes-action-against-amazon-enrolling-consumers-amazon-prime-without-consent-sabotaging-their

[34] https://www.ftc.gov/system/files/ftc_gov/pdf/amazon-rosca-public-redacted-complaint-to_be_filed.pdf

[35] prior to January 2019

[36] https://www.ftc.gov/system/files/ftc_gov/pdf/CK%20Complaint%209-1-22%20%28Redacted%29.pdf

[37] https://www.ftc.gov/legal-library/browse/cases-proceedings/2223087-epic-games-inc-us-v

[38] https://www.ftc.gov/business-guidance/blog/2022/12/record-setting-ftc-settlements-fortnite-owner-epic-games-are-latest-battle-royale-against-violations

[39] https://www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations

[40] https://www.ftc.gov/news-events/news/press-releases/2011/10/peer-peer-file-sharing-software-developer-settles-ftc-charges

the action bars Frostwire from "using default settings that would share consumers' files and requires it to provide free upgrades to correct the unintended sharing."[41]

Recently, the FTC alleged that GoodRx[42] and BetterHelp[43] shared personal health information to target users with ads. In both cases, the Commission alleged that the companies automatically collected and shared health data for advertising purposes. The stipulated orders resolving those cases ban the companies from sharing consumer personal information for advertising, directs third parties to delete ill-gotten data, and requires the companies to limit their data retention. The orders also contain a definition of "Affirmative Express Consent" that is designed to prevent companies from employing dark patterns to get consent.

The third area of exploitation are company decisions elevated by information asymmetries. The product design and implementation decisions made by companies, do not just have short term, innocuous effects.

- In the Amazon Alexa matter, the complaint alleged that Amazon's popular voice assistant kept voice and location data indefinitely, prevented parents from deleting data, and put user data at risk which "sacrificed privacy for profits."[44] The stipulated order required Amazon to delete inactive accounts of children and mandated data deletion schedules.
- Dominant firms with vast resources can further entrench their market power through licenses to copyrighted proprietary data.[45] In a filed a comment with the US Copyright Office on generative AI and the creative economy, FTC Staff identified that "conduct that may violate the copyright laws [...] may also constitute an unfair method of competition or deceptive practice, especially when the copyright violation deceives consumers, exploits a creator's reputation or diminishes the value of their work, or reveals private information."

And beyond individual matters, the FTC continues to apply approaches and our tools through rulemakings and policy statements. The agency proposed changes[46] to the Negative Option Rule (also known as the "Click to Cancel" rule) which includes: simple cancellation mechanisms, new requirements before making additional offers, and annual reminders before automatic renewal.[47] The FTC proposed changes to the Children's Online Privacy Protection Rule (COPPA Rule) that would require targeted advertising to be off by default, limit push notifications, restrict surveillance in schools and strengthen data security.[48]

---

[41] https://www.ftc.gov/news-events/news/press-releases/2011/10/peer-peer-file-sharing-software-developer-settles-ftc-charges
[42] https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising
[43] https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-gives-final-approval-order-banning-betterhelp-sharing-sensitive-health-data-advertising
[44] https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever
[45] https://www.ftc.gov/news-events/news/press-releases/2023/11/InCommentSubmittedtoUSCopyrightOfficeFTCRaisesAIrelatedCompetitionandConsumerProtectionIssuesStressingThatItWillUseItsAuthoritytoProtectCompetitionandConsumersinAIMarkets
[46] https://www.ftc.gov/system/files/ftc_gov/pdf/NegOptions-1page.pdf
[47] https://www.ftc.gov/news-events/news/press-releases/2023/03/federal-trade-commission-proposes-rule-provision-making-it-easier-consumers-click-cancel-recurring
[48] https://www.ftc.gov/news-events/news/press-releases/2023/12/ftc-proposes-strengthening-childrens-privacy-rule-further-limit-companies-ability-monetize-childrens

Conclusion

So, how might technologists at the agency strengthen and support the FTC's mission? The first is an acknowledgment that each layer of the tech stack — from the front-end user interface to the data, models, and hardware of a product or service — is a manifestation of a company's core business model and incentives.

Notice and choice is a form of design pattern and a policy framework - which has failed to actually protect user privacy. It has enabled industry to hoover up data to propel the surveillance economy and led to a critical need for law enforcers to investigate dark patterns in areas where companies exploit consumer vulnerabilities: incremental daily cuts, systemic disadvantages, and power asymmetries.

The FTC has weathered many new seasons of technological change - and this moment is no different. We will continue to use our tools to ensure that companies do not trick, bully or coerce consumers.

***

A special thanks: Cases and investigations exist today due to the decades of law enforcement by my colleagues in the Commission. I want to thank Samuel Levine — and my colleagues who helped review this post: Alex Gaynor, Amritha Jayanti, Noam Kantor, Wells Harrell and Bikram Bandy.