"SOMETHING IS HAPPENING HERE BUT YOU DON'T KNOW WHAT IT IS. DO YOU, MRS. JONES?" DARK PATTERNS AS AN ANTITRUST VIOLATION

BY JAY L. HIMES & JON CREVIER[1]

1 Title adapted from Bob Dylan, Ballad of a Thin Man (1965). Jay Himes is a former co-chair of Labaton Sucharow LLP's Antitrust Practice Group, and also a former Antitrust Bureau Chief, Office of the Attorney General of the State of New York. Jon Crevier is an associate at the Labaton firm.

Visit www.competitionpolicyinternational.com for access to these articles and more!

"Something Is Happening Here but You Don't Know What It Is. Do You, Mrs. Jones?" Dark Patterns as an Antitrust Violation

By Jay L. Himes & Jon Crevier

Internet users surfing from one website to another, or using various web-enabled applications, regularly encounter "dark patterns" — web-design choices that trick users into unknowingly providing more time, money, or attention than they realize. Dark patterns thus manipulate users, impairing their ability to exercise free choice and to express their actual preferences. Their use on the web is pervasive. Moreover, as artificial intelligence develops and as the "internet of things" rolls out, the ability and opportunity to manipulate and exploit consumers via dark patters will, predictably, increase. This article discusses various dark pattern techniques and explains the conditions accounting for their frequency of use in the digital space. Legislation prohibiting dark patterns and litigation challenging them as deceptive acts or practices are becoming available. However, dark patterns also have anti-competitive consequences, as they shift surplus from customers to suppliers, while also raising rivals' costs to compete. Accordingly, antitrust enforcement should also be available to remedy these ubiquitous and pernicious online practices.

As internet users surf from one website to another, or use web-enabled applications, they regularly — and unknowingly — encounter "dark patterns" — "the often unseen web-design choices that trick users into handing over more time, money, or attention than they realize."[2] Dark pattern techniques "make it difficult for users to express their actual preferences or . . . manipulate users into taking actions that do not comport with their preferences or expectations. Examples of dark patterns abound in privacy and security."[3] As Acting FTC Chair Rebecca Slaughter recently said in keynoting an agency workshop — Bringing Dark Patterns to Light — "[w]e increasingly see companies using dark patterns to manipulate people into giving up their data, which is then sold, aggregated, analyzed, and used to target advertising and manipulate future purchases and behavior . . . . We also see dark patterns used more directly to manipulate consumer behavior."[4]

This state of affairs is only likely to get worse: "[e]merging methods of big data present a new and vastly more efficient way to identify cognitive bias by attempting to pinpoint profitable anomalies."[5] As artificial intelligence develops apace and as the "internet of things" rolls out, the ability and opportunity to manipulate and exploit consumer biases will, predictably, increase — unless we take action to stop it.

Below, we first explain what dark patterns are and why they are used so frequently online. After that, we address the impact of dark patterns on user choice and online engagement. Finally, we discuss various approaches to attack dark patterns. Legal action grounded in prohibition of false or deceptive acts or practices, as well as legislation and regulatory intervention, are two approaches. Another, however, is antitrust enforcement, as dark patterns have competitive consequences. Dark patterns shift surplus from customers to suppliers and raise rivals' costs to persuade customers to switch to their platforms. Accordingly, existing antitrust law is nimble enough to tackle dark patterns.

2 Sidney Fussell, The Endless, Invisible Persuasion Tactics of the Internet, The Atlantic (Aug. 2, 2019), https://www.theatlantic.com/technology/archive/2019/08/how-dark-patterns-online-manipulate-shoppers/595360/.

3 Stigler Ctr., Stigler Comm. on Digital Platforms, Final Report, at 210 (2019), Stigler-Committee-on-Digital-Platforms-Final-Report.pdf (publicknowledge.org) (" Stigler Center Report"); see also *id.* at 12-13, 237-55.

4 FTC, Bringing Dark Patterns to Light, Workshop (Apr. 29, 2021), at 1-2, (transcript available at https:// www.ftc.gov/system/files/documents/public_events/ 1586943/ftc_darkpatterns_workshop_transcript.pdf.) (" FTC Workshop").

5 Ryan Calo, Digital Market Manipulation, 82 Geo. Wash. L. Rev. 996, 1010 (2014).

I. WHAT ARE DARK PATTERNS?

Dark patterns "are not mistakes. They're carefully crafted with a solid understanding of human psychology, and they do not have the user's interests in mind."[6] Dark patterns draw on recognized human behavioral phenomena to "nudge" users in the direction sought by the online company even though this direction might not otherwise be preferred by the user or in the user's best interests. The "roach motel" technique is one example: "The design makes it very easy for you to get into a certain situation, but then makes it hard for you to get out of it (e.g. a subscription)."[7] For example, "Amazon makes it exceedingly easy for consumers to sign up for Prime, only requiring a couple of clicks on a prominent advertising banner. This stands in stark contrast to the process of ending the subscription."[8] Then, the prime member is "faced with a large number of hurdles, including complicated navigation menus, skewed wording, confusing choices, and repeated nudging," which "takes at least seven clicks to complete. . . ."[9]

Harry Brignull, a UK web designer who coined the expression "dark patterns," identifies other common techniques:[10]

- Trick questions: "When glanced upon quickly the question appears to ask one thing, but when read carefully it asks another thing entirely."
- Sneak into Basket: On your way to online checkout, an additional item is put into your basket, "often through the use of an opt-out radio button or checkbox on a prior page."
- Privacy Zuckering: Tricks that cause the user to share more information than really intended.
- Price Comparison Prevention: Design techniques that make it hard to compare the prices of items, "so you cannot make an informed decision."
- Misdirection: Design techniques that "purposefully focus[…] your attention on one thing in order to distract your attention from another."
- Hidden Costs: At the final checkout step, unexpected charges appear, such as delivery charges or taxes.
- Bait and Switch: "You set out to do one thing, but a different, undesirable thing happens instead."
- Confirmshaming: "[G]uilting the user into opting" in, by wording the opt-out option "in such a way as to shame the user into compliance." (For example, "No thanks, I'm not into savings"[11]).
- Disguised Ads: Camouflaging ads "as other kinds of content or navigation, in order to get you to click on them."
- Forced Continuity: Once a free trial ends, "your credit card silently starts getting charged without any warning. In some cases this is made even worse by making it difficult to cancel the membership."

---

6 Harry Brignull, Dark Patterns: inside the interfaces designed to trick you, The Verge, (Aug. 29, 2013), https://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you. See also Daniel Susser, Beate Roessler & Helen Nissenbaum, Technology, autonomy, and manipulation, 8 Internet Pol'y Rev. 1, 7 (Issue 2 2019) (dark patterns are "design strategies that exploit users' decision-making vulnerabilities to nudge them into acting against their interests (or, at least, acting in the interests of the website or app)"), https://policyreview.info/articles/analysis/technology-autonomy-and-manipulation.

7 Harry Brignull, Dark Patterns: Roach Motel, https://www.darkpatterns.org/types-of-dark-pattern/roach-motel.

8 Norwegian Consumer Council, You Can Log Out, But You Can Never Leave 29 (Jan. 14, 2021), https://fil.forbrukerradet.no/wp-content/uploads/2021/01/2021-01-14-you-can-log-out-but-you-can-never-leave-final.pdf.

9 *Id.* at 3, 11.

10 Harry Brignull, Dark Patterns: Types of Dark Patterns, https://www.darkpatterns.org/types-of-dark-pattern. See also Australian Competition & Consumer Commission (ACCC) Digital Platforms Inquiry: Final Report, at 422 et seq. (§7.7) (Dec. 2018) (discussing design choices and practices that nudge consumers away from less privacy invasive data collection, use, and disclosure) https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf ("ACCC Report"); Jamie Luguri & Lior Jacob Strahilevitz, Shining a Light on Dark Patterns, 13 J. Leg. Anal. 43, 53 (2021) ("Table 1: Summary of existing dark pattern taxonomies"), https://ssrn.com/abstract=3431205.

11 Numerous examples of confirmshaming can be seen at confirmshaming.tumblr.com.

- Friend Spam: You're asked for your email or social media permissions "under the pretense it will be used for a desirable outcome (e.g. finding friends), but then spams all your contacts in a message that claims to be from you."

FTC Commissioner Chopra has similarly noted that "[d]ark pattern tricks involve an online sleight of hand using visual misdirection, confusing language, hidden alternatives, or fake urgency to steer people toward or away from certain choices."[12] An online retailer who — to create a sense of urgency — reports to the potential customer that there is "one in inventory" for an item when that simply is untrue is illustrative.[13] A study of 11,000 online shopping websites identified 1818 instances of dark patterns, falling into 15 types — and, indeed, uncovered third-parties marketing their ability *to enable* dark patterns.[14]

In sum, while varying in form, dark patterns center on two themes: (1) some are deceptive or "information-hiding," thus "deceiving [users] or by delaying the necessary information to them," while others (2) "are asymmetric, covert, or deferentially treating of users, and restrictive."[15] Regardless of the theme, the effect is to "modify the decision space for users" so as to "ultimately influence how users make choices"[16] Notably, dark patterns can affect particular groups — indeed, even particular individuals — differently, and thus cause disparate, rather than uniform, harm.[17]

II. WHY ARE ONLINE DARK PATTERNS SO PREVALENT?

There is a commonsense intuition that probably accounts for the frequency of dark patterns in the online space: "the internal, proprietary research suggests dark patterns generate profits for the firms that employ them."[18] As web designer Brignull told those at the FTC's recent Dark Patterns Workshop:

Imagine if you ran a business and you could press a button to get your customers to spend 21 percent more, it's a no-brainer. Of course you'd press it. And that's the reason why dark patterns exist.[19]

In consequence, "[m]odern online environments are replete with smart, persuasive choice architectures that are designed primarily to maximize financial return for the platforms, capture and sustain users' attention, monetize user data, and predict and influence future behavior."[20] As web designers build dark patterns into their sites, these techniques "undermine consumers' ability to make free and informed choices by making us act against our own interests in favour of the interest of service providers."[21]

---

12 F.T.C., Statement of Commissioner Rohit Chopra, Regarding Dark Patterns in the Matter of Age of Learning, Inc., (Sept. 2, 2020), https://www.ftc.gov/system/files/documents/public_statements/1579927/172_3086_abcmouse_-_rchopra_statement.pdf. See also Anastasia Kozyreva, Stephan Lewandowsky & Ralph Hertwig, 21 Psych. Sci. in the Pub. Int. 103, 111-14 (Issue 3 2020) (discussing persuasive and manipulative techniques, and identifying, as categories of dark patterns, sneaking, urgency, misdirection, social proof, scarcity, obstruction, and forced action), https://journals.sagepub.com/doi/pdf/10.1177/1529100620946707. See also FTC Workshop, *supra* n. 4, at 8-9 (remarks of Arunesh Mathur: identifying dark patterns by their attributes).

13 See generally Stigler Center Report, *supra* n. 3, at 241.

14 Arunesh Mathur, *et al.*, Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites, The Atlantic (Sept. 2019), § 5.1 & Table 1, § 5.2 & Table 2, https://arxiv.org/pdf/1907.07032.pdf.

15 FTC Workshop, *supra* n. 4, at 8 (remarks of Arunesh Mathur).

16 *Id.* at 8. See also Stigler Center Report, *supra* n. 3, at 238 (dark patterns' "central unifying feature is that they are manipulative, rather than persuasive. More specifically, the design choices inherent in dark patterns push users towards specific actions without valid appeals to emotion or reason."). See generally *id.* at 238-42; Norwegian Consumer Council, Deceived By Design, 6-7 (§3.1), 12-39 (§4) (discussing dark patterns created by Facebook, Google, and Microsoft using (1) default settings, (2) cumbersome setting navigation paths, (3) framing, (4) rewards and punishments, (5) forced action and control, (5) illusion of user control) (June 27, 2018), https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

17 See e.g. FTC Workshop, *supra* n. 4, at 2 (remarks of FTC Acting Chair Rebecca Slaughter), 13 (remarks of Kat Zhou & Dr. Katharina Kopp), 25, 29 (remarks of Lior J. Strahilevitz), 44-45, 52 (remarks of Mutale Nkonde), 49-51 (remarks of Drs. Jasmine McNeely & Kelly Quinn), 53-65. (panel discussion of dark patterns directed to children and teens), 84 (remarks of Daniel Kaufman).

18 Luguri, *supra* n. 10, at 45.

19 FTC Workshop, *supra* n. 4, at 7.

20 Kozyreva, *supra* n. 12, at 111 (citation omitted).

21 Norwegian Consumer Council, *supra* n. 8.

III. PERSUASION V.2.0 — OR NOT?

Advertiser persuasion — even deception — is, of course, nothing new. Are digital world dark patterns simply old wine in new wineskins? We, along with many others, think not. "Traditional brick-and-mortar stores and online platforms differ greatly in their advertising and personalization capabilities."[22] Several conditions in the online world coalesce to favor much enhanced resort to dark patterns:

- For one, while websites appear neutral, online companies "design every aspect of the interaction with the consumer."[23] These consumer-facing websites mask how the "interface shapes [the user's] interactions with, and perception of, online content" and cause them to "underappreciate the constructed nature of the information and choices presented . . . ."[24]

- At the same time, online companies are incented to cultivate in the user an "illusion of control" so that "deceptive design is unlikely to be questioned or even noticed."[25] Thus, users "routinely interact with the online environment in an efficient, task-focused, and habitual way," often acting reflexively "based on only a few visual cues" and ignoring "the rest of the screen."[26]

- Also, user activity online lends itself to "A/B testing," a technique in which slight website variants are delivered to subset user groups to determine that variant that results in "more" of the tester's desired response — "gaining more clicks, longer visits, more purchases."[27] "Online experiments allow designers to find the answers with just a few lines of code."[28] The variants can reflect subtle differences: "Yes, it's true that a team at Google couldn't decide between two blues, so they're testing 41 shades between each blue to see which one performs better."[29]

- Using A/B testing and applying computer analytics to massive amounts of data and real-time user activity, online companies can identify user vulnerabilities and exploit the interaction moment not only for groups, but also for individuals — and to deliver personalized ads systematically.[30]

Consequently, opportunities and techniques in the digital space, beyond those available in the brick and mortar world, enable dark patterns to drive decisions that the user otherwise would not make. Further, in the brick and mortar world, a customer can "just say no" to hype and walk away. By contrast, in the digital space, even when the user does not succumb to the dark patterns, the online company still collects valuable user data before the user eventually navigates her way out.[31]

---

22 Stigler Center Report, *supra* n. 3, at 45. See also Margherita Colangelo & Mariateresa Maggiolino, Manipulation of Information as Antitrust Infringement, 26 Colum. J. Eur. L. 63, 64-65 (2020); Kozyreva, *supra* n. 13, at 106-11 (discussing systematic differences between online and offline environments); Luguri, *supra* n. 10, at 103 ("The online environment is different. It is perhaps only a difference of degree, but the degrees are very large. . . . What was once an art is now a science. As a result, consumers' ability to defend themselves has degraded."); FTC Workshop, *supra* n.4, at 35 (remarks of Finn Lutzow-Holm Myrstad: "The experience . . . from a brick and mortar stores . . . [is] taken up to another scale and can also do this in real time and really see how it works and how different consumer groups react to different types of dark patterns.").

23 Calo, *supra* n. 5, at 1004.

24 Lauren E. Willis, Deception by Design, 34 Harv. J. of Law & Tech. 116, 132 (2020).

25 *Id.* at 133; ACCC Report, *supra* n. 10, at 423 (§7.7.2); Kozyreva, , *supra* n. 12, at 104("the Internet is . . . , notwithstanding appearances, a highly controlled environment," in which user access "is regulated by algorithms and design choices made by corporations in pursuit of profits and with little transparency or public oversight.").

26 Willis, *supra* n. 24, at 132, 138; Susser, *supra* n. 6, at 7-8 (that digital technology has "become invisible to us — simply through frequent use and habituation — means the influences they facilitate are often hidden, and thus potentially manipulative. . . . And the more we become habituated to these systems, the less attention we pay to them.").

27 Brian Christian, The A/B Test: Inside the Technology That's Changing the Rules of Business, Wired (Apr. 25, 2012), https://www.wired.com/2012/04/ff-abtesting/. See generally Willis, *supra* n. 24, at 116, 127-28 & n. 52; Calo, *supra* n. 5, at 1015 & n. 114.

28 Arvind Narayanan, Arunesh Mathur, Marshini Chetty & Mihir Kshirsagar, Dark Patterns: Past, Present, and Future, 18 ACM Queue 67, 76 (Issue 2 2020).

29 Douglas Bowman, Goodbye, Google (Mar. 20, 2009), https://stopdesign.com/archive/2009/03/20/goodbye-google.html. See also FTC Workshop, *supra* n. 4, at 38 (remarks of Dr. Jonathan Mayer: company tested different shades of grey "to see how that changed user behavior with the consent notice.")

30 See generally Willis, *supra* n. 25, at 132, 142-45; Susser, *supra* n. 6, at 6-7; Calo, *supra* n. 5, at 1021-22; FTC Workshop, *supra* n. 4, at 13-14 (remarks of Dr. Katharina Kopp); Stigler Center Report, *supra* n. 3, at 242.

31 FTC Workshop, *supra* n. 4, at 45-46 & 46-47 (remarks of Drs. Jasmine McNeeley & Kelly Quinn).

IV. HOW BAD IS IT — REALLY?

In a recent study, researchers invited random participants to answer survey questions relating to their privacy views, after which they were offered a data protection plan.[32] A control group could decline the plan in a simple yes/no screen, while two other participant groups were subjected to either "mild" or "aggressive" dark patterns. Those subject to mild dark patterns accepted the protection plan 2.3 times more often than the control group, and those subject to aggressive dark patterns 3.7 times more often.[33] As these study results confirm, "we're seeing dark patterns proliferate because they're extremely effective."[34]

In a second study, these researchers probed more closely the impact of particular forms of dark patterns. Some "had a striking effect on consumer choice, others had little to no effect."[35] Of those exposed to a trick question, only half of those who in fact accepted the protection plan *believed* they had done so.[36] The trick worked: "not only were consumers manipulated into selecting acceptance, but they didn't understand that they had been manipulated and signed up for something that they didn't actually want to sign up for."[37] The researchers thus concluded: "*dark patterns are strikingly effective in getting consumers to do what they would not do when confronted with more neutral user interfaces.*"[38]

The 2020 House subcommittee report quoted from this research: "[dark patterns] are harming consumers by convincing them to surrender cash or personal data in deals that do not reflect consumers' actual preferences and may not serve their interests. There appears to be a substantial market failure where dark patterns are concerned — what is good for ecommerce profits is bad for consumers."[39] "Market failure" is both a consumer protection and an antitrust concern. Dark patterns are deployed to encourage continued user engagement with the online company, and user engagement equates to more data captured. For already dominant platforms, more data fortifies barriers to entry, thus perpetuating the feedback loop, driven by economies of scale and scope, that entrenches dominance.[40] But even for non-dominant players, by maintaining user site engagement, dark patterns dampen competition.

32 Luguri, supra n. 10,. See generally FTC Workshop, supra n. 4, at 21-30 (remarks of Lior Jacob Strahilevitz: describing the study).

33 Luguri, *supra* n. 10, at 64.

34 FTC Workshop, supra n. 4, at 25 (remarks of Lior Jacob Strahilevitz).

35 Luguri, *supra* n. 10, at 75.

36 *Id.* at 78 (emphasis in original).

37 FTC Workshop, *supra* n. 4, at 28 (remarks of Lior Jacob Strahilevitz).

38 Luguri, *supra* n. 10, at 46.

39 House Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary, Investigation of Competition in Digital Markets, Majority Staff Report and Recommendations 53 (2020) (footnote omitted) (quoting Luguri, *supra* n. 10, at 81-82).

40 See FTC Workshop, *supra* n. 4, at 1 (remarks of Acting FTC Rebecca Slaughter).

V. DECEPTIVE BY DESIGN

The dark patterns practiced on users today are akin to "subliminal" advertising used in television or radio broadcasts. "Subliminal" advertising is "any technique whereby an attempt is made to convey information to the viewer by transmitting messages below the threshold level of normal awareness."[41] Thus, subliminal ads "bypass the viewer's conscious mind entirely and lodge in the subconscious as fully formed and conclusory thoughts. They are, therefore, inconsistent with the goal of rational consumer choice and should be condemned as an unfair consumer practice."[42] Accordingly, in 1974, the Federal Communications Commission declared subliminal ads "contrary to the public interest. Whether effective or not, such broadcasts clearly are intended to be deceptive."[43] And although the case law is limited, courts have held that subliminal messages are "akin to false and misleading commercial speech" and thus subject to "little, if any, first amendment constitutional protection."[44]

Dark patterns are subliminal ads on steroids. Subliminal ads at least have to wait for viewer-groups before they can be used. By contrast, in the digital space, firms "choose when to approach consumers, rather than wait until the consumer has decided to enter a market context."[45] Dark patterns thus can be delivered whenever a user surfs the internet, and they can be adapted for individual users, specifically targeted to manipulate that particular user's decision-making process *at the very moment approached*.[46]

For example, digital companies have learned techniques to produce neuro-chemical responses in users, stimulating dopamine in the brain, to "hook" them on engaging the online site. Dopamine "is a neurotransmitter that rewards the body when a positive event occurs randomly."[47] As Sean Parker, Facebook's early president, has stated publicly, the company developed features such as the "like" button to give users "a little dopamine hit" that would help Facebook "consume as much of [the user's] time and conscious attention as possible."[48] Apple executive Eddie Cue similarly wrote internally: "[g]etting customers using our stores . . . is one of the best things we can do to get people hooked to the ecosystem."[49] Thus, "[t]ech companies understand what causes dopamine surges in the brain and they lace their products with 'hijacking techniques' that lure us in and create 'compulsion loops.'"[50] The more time the user spends on a company's website, the more data the company amasses, and the greater is its ability to target and manipulate.[51] "[P]ersonal data is the fuel of the manipulation process."[52]

---

41 Broadcast of Information by Means of 'Subliminal Perception' Techniques, 44 F.C.C. 2d 1016, 1017 (1974) (quoting the NAB Television Code).

42 Neil W. Averitt & Robert H. Lande, Consumer Sovereignty: A Unified Theory of Antitrust and Consumer Protection Law, 65 Antitrust L.J. 713, 740 (1997).

43 44 F.C.C. at 1017. See generally Marisa E. Main, Simply Irresistible: Neuromarketing and the Commercial Speech Doctrine, 50 Duq. L. Rev. 605, 615-16 (2012).

44 *Waller v. Osbourne*, 763 F. Supp. 1144, 1148 (M.D. Ga.1991), *aff'd without op.*, 958 F.2d 1084 (11th Cir.1992), *cert. denied*, 506 U.S. 916 (1992). See also *Vance v. Judas Priest*, 1990 WL 130920, at *25 (D.C. Nev. Aug. 24, 1990) ("not entitled to First Amendment protection") (appendix: summary judgment ruling). *Cf.* Ramsi A. Woodcock, The Obsolescence of Advertising in the Information Age, 127 Yale L. J. 2270, 2330 (2018) (footnote omitted) ("advertising that is purely persuasive, in the sense that it conveys no useful product information, is not protected by the First Amendment."); Calo, *supra* n. 5, at 1040 ("the collection of data for an unexpected purpose, the potential of digital market manipulation to mislead, or the possibility of undue influence" militate against First Amendment protection).

45 *Id.* at 1004.

46 See generally Susser, *supra* n. 6.

47 Gregory Day & Abbey Stemler, Are Dark Patterns Anticompetitive?, 72 Ala. L. Rev. 1, 12 (2020).

48 Olivia Solon, Ex-Facebook president Sean Parker: site made to exploit human 'vulnerability', The Guardian, (Nov. 9, 2017), https://www.theguardian.com/technology/2017/nov/09/facebook-sean-parker-vulnerability-brain-psychology. See generally *Stigler Center Report, supra n. 3, at 64-66 ("Online Exploitation and Addiction"); Day, supra* n. 47, at 21-22.

49 Dorothy Atkins, Apple Wanted App Users 'Hooked,' Exec's 2013 Email Reveals, Law360 (May 11, 2021), https://www.law360.com/articles/1383530/apple-wanted-app-users-hooked-exec-s-2013-email-reveals.

50 David Brooks, How Evil Is Tech? NY Times (Nov. 20, 2017), https://www.nytimes.com/2017/11/20/opinion/how-evil-is-tech.html. See also Simon Parkin, Has dopamine got us hooked on tech?, The Guardian (Mar. 4, 2018), https://www.theguardian.com/technology/2018/mar/04/has-dopamine-got-us-hooked-on-tech-facebook-apps-addiction.

51 Fiona M. Scott Morton & David C. Dinielli, Roadmap for an Antitrust Case Against Facebook (June 2020), at 4-5 ("Facebook Roadmap"). See also FTC Workshop, *supra* n. 4 , at 14 (remarks of Dr. Katharina Kopp: describing the objectives of dark patterns: (1) more "sales and revenue," (2) more user "engagement and attention, which may lead to harms of addiction," and (3) more "data use and collection.").

52 Tal Zarsky, Privacy and Manipulation in the Digital Age, 20 Theoretical Inquiries in Law 157, 186 (2019) (footnote omitted), https://din-online.info/pdf/th20-1-8.pdf.

Because data is so valuable, digital companies "are not incentivised to encourage consumers to opt out" of collection, use, or disclosure of their data; to the contrary, to avoid outward migration or product substitution, online companies seek "to convey an impression that they offer consumers significant control" over the data they're providing.[53] Moreover, companies are receptive to dark patterns "simply because a design that tricks users into doing something is likely to achieve more conversions [that is, user responses] than one that allows users to make an informed decision."[54] And on the user side, "[g]rowing reliance on digital tools in all parts of our lives — tools that constantly record, aggregate, and analyse information about us — means we are revealing more and more about our individual and shared vulnerabilities. . . . And the more we become habituated to these systems, the less attention we pay to them."[55]

Thus, dark patterns not only emerge, they also propagate to become "a regular part of the fabric of everyday experience."[56] They are particularly effective when used to nudge users to choose an offered default option. Users are disinclined to depart from a default they are offered or that they select (albeit through nudging).[57] This "default" or "status quo" bias is well-recognized: "individuals generally stick with the default choices they are presented with."[58] Dark patterns can themselves reinforce the bias. And this behavioral propensity means that nudging the user towards selecting the default offered entrenches the digital company's position.[59] By exploiting the user's default bias, "consumers make decisions they might not make with fuller consideration."[60]

VI. ZERO-PRICE EFFECTS

It is commonplace to hear talk of the many "free" services available on the internet. But, of course, nothing's "free." More accurately, many digital companies offer their products to users at a "zero-price" and thus must develop revenue from another source. In the digital space, online companies typically sell user access to advertisers and sometimes also deliver ads to content providers, referred to as "publishers," who offer "billboard" space on their website, from which a digital intermediary such as Google takes a cut of the payment to the publisher. This business model in turn requires the digital company to collect user data that can be analyzed to allow targeted advertising to be delivered to users, who pay for the zero-price product by providing their data. Further, as the user engages with an advertiser or publisher, the user's payment in data harvested increases. More user data permits more granular data analysis, leading to improved ad targeting. And improved ad targeting enables the company to charge more to its advertisers, as well as to publishers, for delivering ads. To enable ad dollars to flow at increasing rates, the digital company is incented to keep the user engaged on its website or on linked sites, thereby gathering as much data as it can.

Dark patterns can be used to maintain this user engagement and — equally important — to improve ad targeting that results in purchases users might not otherwise make.[61] Applying data analytics to large data sets, online businesses can "explore every nook and cranny of consumers' many behavioral shortcomings and biases in real time. Framing, nudges, and defaults can direct a consumer to the choice that is

53 ACCC Report, *supra* n. 10, at 423 (§7.7.2).

54 Brignull, *supra* n. 6,. See also Brice Berdah, Dark patterns: submission by design?, UX Collective, Apr. 15, 2019, ("If you A/B test an honest, non-deceptive form versus a dark pattern filled one, the second one will certainly land more conversions."), https://uxdesign.cc/dark-patterns-submission-by-design-6f61b04e1c92.

55 Susser, *supra* n. 6.

56 *Id.*

57 See e.g. Jason Furman, Unlocking Digital Competition — Report of the Digital Competition Expert Panel 36 (Mar. 2019) (footnote omitted); ACCC Report, *supra* n. 10, at 431 (§7.7.5).

58 Competition & Markets Authority, Online Platforms and Digital Advertising: Market Study Final Report (July 1, 2020), at204 (¶ 4.205) ("CMA Final Report"); see also *id.* 13-15 (¶¶ 31-40) ("Consumer decision making and the power of defaults"). *See also* Stigler Center Report, *supra* n. 3, at 8 ("Consumers tend to stick with default options."); Furman, *supra* n. 57.

59 Stigler Center Report, *supra* n. 3, at 42. See also ACCC Report, *supra* n. 10, at 10 ("Consumer behaviour favours the use of incumbents, particularly those with strong brands. The operation of default settings further entrenches the market power of incumbents and increases the barriers to entering these markets."); CMA Final Report, *supra* n. 58, at 13-15 (¶¶ 31-40) ("Consumer decision making and the power of defaults").

60 *Id.* at 204 (¶ 4.205).

61 See generally Facebook Roadmap, *supra* n. 51, at 4-5 (discussing Facebook); Willis, *supra* n. 24, at 116, 121-23; Stigler Center Report, *supra* n. 3, at 11, 210-12, 246-48.

most profitable for the platform."[62]

Offering online products at zero-price has another significant effect. It disables price as a signal for perceived product attractiveness: "[w]hen facing a zero-money price, and when quality is difficult to observe, consumers are not receiving salient signals about the social value of their consumption because the price they believe they face [that is, "zero"] does not reflect the economics of the transaction, and they are ignorant of those numbers."[63] Simply put, "there is no analogue to a 'price tag' for attention (or information) costs."[64] Moreover, while the company harvesting the user's data knows it's receiving something valuable, how valuable isn't all that clear because analytics need to be applied to add value and because harvested data may be used in ways not even apparent when collected.[65]

Digital companies are, therefore, incented to collect ever-increasing amounts of data. Dark patterns help achieve, maintain, and augment the user engagement that enables data collection.

VII. THE CURRENT LEGAL ENVIRONMENT

Deception is the core feature of dark patterns. Therefore, dark patterns should be actionable under federal and state law barring false, deceptive, or unfair practices.[66] A handful of FTC cases have addressed dark pattern techniques, albeit not using this terminology itself.[67] Ironically, however, "the proliferation and sheer variety of dark patterns on its own makes it more difficult for government enforcers to effectively identify the most severe offenders and to address these offenders through targeted enforcement actions."[68] Accordingly, there is a role for private enforcement, and many private cases that explicitly plead deceptive "dark patterns" are pending. All are in their early stages so that the court has not ruled on the claim's legal sufficiency.[69] Deception theory aside, contract law concepts could also be applied to void user agreements elicited using dark patterns.[70]

---

62 *Id.* at 30. See also FTC Workshop, supra n. 4, at (remarks of Ryan Calo: "the idea of persuasion profiling is . . . how do you find out what persuades a person, and then leverage that in real time"); Testimony of Gene Kimmelman Before the Senate Judiciary Committee, Subcommittee on Antitrust, Competition Policy and Consumer Rights 8 (Mar. 10, 2020) ("Powerful incumbent platforms may also make design choices to exacerbate this inclination [the default bias nudging people to stay put].") (footnote omitted) , https://www.judiciary.senate.gov/imo/media/doc/Kimmelman%20Testimony.pdf.

63 Stigler Center Report, *supra* n. 3, at 67. See also CMA Final Report, *supra* n. 58, at 13 (¶ 32) ("default behaviour by consumers has had a profound impact on the shape of competition in both search and social media.") (emphasis deleted).

64 John Newman, Antitrust in Zero-Price Markets: Foundations, 164 U. Penn. L. Rev. 149, 179 (2015).

65 Katharine Kemp, Concealed data practices and competition law: why privacy matters, 16 Euro. Comp. J. 628, 642-43 (2020).

66 See e.g. Section 5 of the FTC Act, 15 U.S.C. § 45(a), which declares unlawful "unfair or deceptive acts or practices in or affecting commerce." The elements of deception are "[1] a representation, omission, or practice, that [2] is likely to mislead consumers acting reasonably under the circumstances, and [3], the representation, omission, or practice is material." *FTC v. LeadClick Media, LLC*, 838 F. 3d 158, 168 (2d Cir. 2016) (cleaned up). See also Luguri, *supra* n. 10, at 83-91.

67 *Federal Trade Commission v. LeadClick Media, LLC*, 838 F. 3d 15 (2d Cir. 2016) (finding deception where company created bogus customer reviews that it posted on fake online news sites); *Federal Trade Commission v. AMG Capital Management*, 910 F.3d 417 (9th Cir. 2018) (finding deception where company made rejecting automatic renewal onerous), *rev'd on other grounds*, ___U.S. ___, No. 19-508 (Apr. 22, 2021); *Fanning v. Federal Trade Commission*, 821 F. 3d 164 (1st Cir. 2016) (finding deception where the vast majority of online user profiles were generated by defendant, not by actual users). See also Complaint, *FTC v. FrostWire LLC*, No. 11-cv-23643-DLG (S.D. Fla. Oct. 12, 2021) (file-sharing set-up procedure, settings and interface were deceptive); Complaint, *Federal Trade Commission v. Age of Learning, Inc.*, 20-cv-07996 (C.D. Cal. Sept. 1, 2020) (membership interface, automatic renewal term, and cancellation process were deceptive); Complaint, *United States v. Facebook Inc.*, 19-cv-02184 (D.D.C. July 24, 2019) (action to enforce FTC consent decree based, in part, on deceptive collection of user data).

68 FTC Workshop, *supra* n. 4, at 72 (remarks of Jennifer Rimm). See also *id.* at 74 (remarks of Lauren E. Willis: proliferation of online marketing techniques, microtargeting, and automation of website display all can be a barrier to effective enforcement actions).

69 See e.g. Third Amended Complaint ¶¶ 44-45, *Nichols v. Noom Inc.*, Docket No. 1:20-cv-03677 (S.D.N.Y. Jan. 29, 2021), ECF 174 ("Noom's business model is predicated upon the 'Hidden Subscription Dark Pattern,' which "Noom augments . . . with numerous other Dark Pattern design techniques," including mental fatigue, trick wording, and roach motel.); Complaint at ¶ 21, *Mendez v. LinkedIn Corp.,* Docket No. 21CV378575 (Cal. Super. Ct. Mar 24, 2021) (LinkedIn uses "various types of dark patterns, including but not limited to 'interface interference' and 'preselection,' 'roach motel, 'misdirection,' and 'forced continuity' in order to prevent user unsubscription").

70 Luguri, *supra* n. 10, at 47-48, 92-97.

In addition, dark patterns have captured the attention of federal and state legislators. Perhaps not surprisingly, California is in the forefront. The California Consumer Privacy Act[71] provides that "dark pattern" means "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, as further defined by regulation."[72] The law further provides that authorization on data use "obtained through use of dark patterns does not constitute consent."[73] Regulations issued under the law give Californians the right to opt-out of sale of their personal information by online companies that collect it, and include, as part of the new rules, provisions banning dark patterns that otherwise could impair exercise of the opt-out right. As the new regulations took effect, then-Attorney General Xavier Becerra said: "These protections ensure that consumers will not be confused or misled when seeking to exercise their data privacy rights."[74] Proposed legislation in Washington State is virtually identical.[75]

Federal legislation may also be in the offing. During the last congressional term, Senators Warner and Fischer introduced the bipartisan Deceptive Experiences to Online Users Reduction (DETOUR) Act.[76] The Act sought to prohibit websites from using dark patterns that trick consumers into handing over their personal data. Among other things, the DETOUR Act would make it unlawful "to design, modify, or manipulate a user interface with the purpose or substantial effect of obscuring, subverting, or impairing user autonomy, decision-making, or choice to obtain consent or user data."[77] The Act would also enable creation of a self-regulatory, professional standards body to "develop, on a continuing basis, guidance and bright-line rules" for platforms on dark patterns design practices,[78] and further would cement the FTC to act as a regulatory enforcer.[79] The bill died upon conclusion of the 116th Congress, However, the bill's sponsors plan to reintroduce the DETOUR Act in the 117th Congress."[80]

Antitrust enforcement is yet another means to rein in dark patterns.

71 Cal. Civ. Code §§ 1798.100 to 1798.199 (CCPA).

72 *Id.* §1798.140(l).

73 *Id.* §1798.140(h).

74 Press Release, Attorney General Becerra Announces Approval of Additional Regulations That Empower Data Privacy Under the California Consumer Privacy Act (Mar. 15, 2021), https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-approval-additional-regulations-empower-data. See California Privacy Act Regulation §999.315(h).

75 Wash. S.5062-S2, §101 (6) & (10).

76 The Deceptive Experiences to Online Users Reduction Act (DETOUR), S.1084, 116th Cong., 1st Sess. §3(a)(1)(A) (Apr. 9, 2019). See also H.R.8975, 116th Cong., 2nd Sess. (Dec. 16, 2020).

77 *Id.* at §3(a)(1)(A).

78 *Id.* at §3(c)

79 *Id.* at §3(d)

80 FTC Workshop, *supra* n. 4, at 4 (remarks of Rep. Lisa Blunt Rochester). See also Sara Morrison, Dark patterns, the tricks websites use to make you say yes, explained, Vox (Apr. 1, 2021), https://www.vox.com/recode/22351108/dark-patterns-ui-web-design-privacy.

VIII. ANTITRUST ENFORCEMENT DIRECTED TO DARK PATTERNS

Dark patterns make the worst out of an already bad situation. "Dark patterns cause consumers to pay a higher data price than they would freely choose."[81] Essentially, users are tricked into overpaying with their data and attention. Further, dark patterns typically create other transaction costs, such as increased user on-site time or attention. Thus, they produce market waste and distortion.[82] By the same token, users pay a quality-adjusted price that is higher than it would be if they weren't deceived. A company's ability to over-charge users in this manner, without causing them to switch to substitutes, reflects company market power and reduces consumer surplus.[83]

In the U.S., if the company has a large enough market share, dark pattern use may constitute unlawful acquisition or maintenance of monopoly power. The anti-competitive conduct consists of secretly shaping, and thus exploiting, consumer choice — the very antithesis of competing on the basis of product merit.[84] In the EU and other jurisdictions, the company's conduct may constitute abuse of dominance or unlawful exploitive conduct.[85] For a Sherman Act §1 claim, the restraint must result from agreement by two or more participants, but conceivably the user itself could satisfy this plurality requirement, particularly when the website designer requires user adherence to terms of service or elicits a product purchase by the user.[86]

Moreover, actual and potential rivals face enhanced barriers to entry, caused by the first-mover's ability to exploit its user base. Where a digital company employs dark patterns to assure user attention and data-delivery, the result is better ad targeting, for which advertisers and content providers will pay the digital company more. Rivals will have to offer advertisers and content providers better terms than they would have to offer if dark patterns were not used to skew user choice and engagement. The first mover's position is reinforced not only by these network effects (often reflected in both economies of scale and scope), but also by the zero-price feature of many online products. When a product is offered at zero-price, to compete a rival must offer a demonstrably more attractive product — one providing identifiably better quality or more desirable product features.[87] Moreover, when, using dark patterns, a tech company captures user attention and increases their engagement with the company's site or on links offered to the user, the ability of rivals to contest the company's offerings is restrained.[88] More attention capture by one company means less opportunity to capture for rivals. Overcoming the asymmetry requires extra effort by the rival.

So, rivals seeking to counter the effects of a competitor's dark patterns on users will incur increased costs to compete. Through means other than competition on the merits of its product, the company raises its rivals' costs to persuade users to switch — anticompetitive conduct under Section 2.[89]

---

81 Facebook Roadmap, *supra* n. 51, at 31; Calo, *supra* n. 5, at 1029-30.

82 Stigler Center Report, *supra* n. 3, at 239.

83 Kemp, supra n. 65, at 656-57; Note, Deception as an Antitrust Violation, 125 Harv. L. Rev. 1235, 1239 (2012).

84 *Cf.* Woodcock, *supra* n. 44, at 2332 (footnote omitted) (false and misleading advertising is denied First Amendment coverage in order "to protect the decision-making processes of consumers . . . by ensuring that consumers can accurately distinguish the attributes of different products and . . . can put their true preferences to work in selecting between those products.") & 2335 (manipulative advertising may be banned because it "interfer[es] with the decision-making process used by consumers to translate preferences into choices").

85 Kemp, *supra* n. 65, at 656-58.

86 See *Monsanto Co. v. Spray-Rite Serv. Corp.*, 465 U.S. 752, 764 n.9 (1984) (to establish an agreement between a supplier and a customer, "evidence must be presented both that the [customer] communicated its acquiescence or agreement, and that this was sought by the [supplier]"). *Cf. Spectators' Commc'n Network Inc. v. Colonial Country Club*, 253 F.3d 215, 222 (5th Cir. 2001) ("[T]here can be sufficient evidence of a combination or conspiracy when one conspirator . . . is enticed or coerced into knowingly curtailing competition by another conspirator who has an anticompetitive motive."); *Eastman Kodak Co. v. Image Technical Servs., Inc.*, 504 U.S. 451, 463 n.8 (1992) (a sale offered only upon a condition is not unilateral conduct outside the scope of Section 1); *Isaksen v. Vermont Castings, Inc.*, 825 F.2d 1158 (7th Cir. 1987) ("The fact that [the plaintiff] may have been coerced into agreeing is of no moment"), *cert. denied*, 486 U.S. 1005 (1988); *Systemcare, Inc. v. Wang Laboratories Corp.*, 117 F.3d 1137, 1138, 1142–43 (10th Cir. 1997) (Section 1 is satisfied where "the seller coerces a buyer's acquiescence" in the transaction; "[t]he essence of section 1's contract, combination, or conspiracy requirement . . . is the agreement, however reluctant, of a buyer to purchase from a seller").

87 See CMA Final Report, *supra* n. 58, at §3.130, Box 2.2 ("The fact that consumers do not pay directly for the platform's services limits their incentives to switch, and means that new entrants must attract users through demonstrably better quality or innovative features, rather than being able to undercut on price.").

88 Colangelo, *supra* n. 22, at 64-65.

89 See e.g. Note, Deception as an Antitrust Violation, 125 Harv. L. Rev. 1235, 1238-39 (2012) (deception both raises rivals' costs directly and deprives them of economies of scale and thus creates inefficiency); Woodcock, *supra* n. 44, at 2313-15 (persuasive advertising can "lure consumers away from [rivals'] innovative products.") (footnote omitted). *Cf.* Facebook Roadmap, *supra* n. 51, at 29 (By offering users obscure privacy settings, Facebook "suppresses competition in quality.").

IX. PERSUASION V. COERCION VIA DARK PATTERNS

Persuasion "means attempting to influence someone by offering reasons they can think about and evaluate."[90] A product supplier may be expected to try to persuade potential customers to use its product. This is, after all, what advertising is supposed to be about. By contrast, "[c]oercion means influencing someone by constraining their options, such that their only rational course of action is the one the coercer intends. . . . [P]ersuading someone to do something is almost always acceptable, while coercing them almost always isn't."[91]

Commercial speech, such as product advertising, is protected by the First Amendment.[92] Accordingly, case law ends to skepticism of antitrust claims arising from representations about products, even when false or misleading. Although such commercial speech lacks redeeming pro-competitive benefits, marketplace counter-speech by rivals, rather than antitrust litigation, is said to be a preferable remedy.[93] This "marketplace of ideas" argument, however, posits that "[t]ruth is expected to outperform lies so long as people *are equipped* to choose it."[94] But this central assumption dissolves when applied to dark patterns — techniques designed and intended surreptitiously to over-ride rational individual decision-making. In these circumstances, dark patterns really amount to *hidden* coercion. And coercion is conduct courts recognize as relevant to establishing unlawful exclusionary conduct by a firm with monopoly, or to proving an unlawful restraint in a rule of reason case based on the totality of the facts.

New York ex rel. Schneiderman v. Actavis plc[95] is illustrative. Actavis, a drug manufacturer, sought to avoid generic competition for sales of its Namenda drug. As the patent for Namenda IR approached expiration, Actavis withdrew the drug from the market and replaced it with a near identical substitute called Namenda XR. Under federal and state pharmaceutical regulatory regimes, Actavis' conduct prevented substitution of a generic version of the drug, and thus required patients to switch from Namenda IR to Namenda ER. The Second Circuit held that Actavis' conduct violated Section 2:

> Defendants' hard switch crosses the line from persuasion to coercion and is anticompetitive. . . . Had Defendants allowed Namenda IR to remain available until generic entry, doctors and Alzheimer's patients could have decided whether the benefits of switching to once-daily Namenda XR would outweigh the benefits of adhering to twice-daily therapy using less-expensive generic IR (or perhaps lower-priced Namenda IR). By removing Namenda IR from the market prior to generic IR entry, Defendants sought to deprive consumers of that choice.[96]

90 Susser, *supra* n. 6, at 4.

91 *Id.*

92 E.g. *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc.*, 425 U.S. at 765 (1976).

93 See e.g. *Schachar v. Am. Acad. of Ophthalmology, Inc.*, 870 F.2d 397, 400 (7th Cir. 1989); *Retractable Tech., Inc. v. Becton Dickinson & Co.*, 842 F.3d 883, 893-97 (5th Cir. 2016) (discussing authorities); 3B Phillip E. Areeda & Herbert Hovenkamp, Antitrust Law: An Analysis of Antitrust Principles and Their Application, ¶ 782b, at 326 (3d ed. 2008) ("There is no redeeming virtue in deception . . . ."). For a contrary view and case law, see Maurice E. Stucke, When a Monopolist Deceives, 76 Antitrust L.J. 823 (2010); *West Penn Allegheny Health System, Inc. v. UPMC*, 627 F.3d 85, 109 & n.14 (3d Cir. 2010) (citing authorities); *Nat. Ass'n of Pharmaceutical Mfrs. v. Ayerst Lab.*, 850 F.2d 904, 916-17 (2d Cir. 1988).

94 Ellen P. Goodman, Digital Information Fidelity and Friction, Knight First Amendment Institute (Feb. 26, 2020) (emphasis added), https://knightcolumbia.org/content/digital-fidelity-and-friction. See also Kozyreva, *supra* n. 12, at 127 ("Human-made, ubiquitous, persuasive, and manipulative designs, which rely on dark patterns and hidden defaults, challenge the human capacity to exercise autonomous and informed choice."); Colangelo, *supra* n. 22, at 65.

95 787 F.3d 638 (2d Cir. 2015). But see Luguri, *supra* n. 10, at 99-101 (suggesting that First Amendment protection may exist for some forms of dark patterns, such a nagging).

96 787 F.3d at 654-55.

Other cases are similar: conduct going beyond persuasion and into coercion can be unlawfully exclusionary.[97] When that coercion is itself covert, it amounts to manipulation and, indeed, where it plants false impressions, to affirmative deception — conduct that is even more pernicious: "we are directed, outside our conscious awareness, to act for reasons we can't recognise, and toward ends we may wish to avoid."[98] Antitrust law should not hesitate to intervene.[99]

The EC's *Google Shopping* case is also instructive. There, Google essentially used a dark pattern in the form of algorithmic bias against competitors.[100] Google's algorithmic bias favored its own comparison shopping sites, while disadvantaging rivals' sites. The company's conduct was "likely to lead to: an increase in the fees payable by retailers using Google Shopping; a consequential increase in the prices to be paid by their customers; a reduction in innovation incentives from both Google Shopping's competing comparison sites and Google Shopping itself; and a reduction of the ability of consumers to access the most relevant comparison shopping services."[101] Thus, Google corrupted the operations of the market by an algorithmic mechanism that favored display of its own sites while degrading placement of rival sites. Both rivals, online retailers, and customers were harmed.

In a similar vein, both U.S. and EU law recognize as anticompetitive collective, undisclosed manipulation of a benchmark used in marketplace pricing. Thus, in *Gelboim v. Bank of America Corp.*,[102] various banks allegedly suppressed the London Inter-Bank Offered Rate (LIBOR) by secretly submitting depressed borrowing rates that violated rate-setting rules. The plaintiffs, holders of various financial instruments affected by the LIBOR rate, "allege[d] that the Banks corrupted the LIBOR-setting process and exerted downward pressure on LIBOR to increase profits in individual financial transactions and to project financial health."[103] The Second Circuit held that the plaintiffs "plausibly alleged both antitrust violation and antitrust injury. . . ."[104] The EC similarly found an antitrust violation involving analogous corruption of the Euro Bond Inter-Bank Offered Rate.[105]

The very point of a benchmark price is to provide a reliable price signal for market participants. If participants knew the price signal lacked reliability, they would cease using the benchmark. So too, if online users knew that dark patterns were corrupting the settings they selected, the features delivered to them, or attractiveness of product displayed to them, they would lose confidence in the benefits of online surfing and purchase offerings.[106]

97 See e.g. *Berkey Photo, Inc. v. Eastman Kodak Co.*, 603 F.2d 263, 287 (2d Cir. 1979) ("so long as [a monopolist's] success was not based on any form of coercion," product design changes are not actionable under section 2); *Mercatus Group, LLC v. Lake Forest Hosp.*, 641 F. 3d 834, 852 (7th Cir. 2011) ("absent an accompanying coercive enforcement mechanism of some kind, even demonstrably false commercial speech is not actionable under the antitrust laws") (cleaned up); *In re Suboxone*, 64 F. Supp. 3d 665, 682 (E.D. Penn. 2014) ("threatened removal" of drug in tablet form "from the market in conjunction with the alleged fabricated safety concerns could plausibly coerce patients and doctors to switch"); *In re Loestrin 24 Fe Antitrust Litig.*,13-md-02472-WES-PAS, slip op. at 97-98 (D.R.I. Aug. 8, 2018) (discussing authorities); *In re Asacol Antitrust Litig.*, No. 15-cv-12730-DJC (D. Mass. July 20, 2016).

98 Susser, *supra* n. 6, at 4.

99 *Cf.* Main, *supra* n. 43, at 629-30 ("the potential for neuromarketing to be overly persuasive, to the point of being coercive or misleading, is significant enough to justify a state's interest in regulating it in order to protect its citizens.").

100 Commission Decision 2017/4444/EC, Relating to proceedings under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the Agreement on the European Economic Area (AT.39740 - Google Search (Shopping)) (June 27, 2017).

101 Colangelo, *supra* n. 22, at 77-78 (citing Google Shopping Decision ¶¶ 589-96).

102 823 F.3d 759 (2d Cir. 2016).

103 *Id.* at 766.

104 *Id.* at 783.

105 Commission Decision, 2013/8512/EC, Relating to proceeding under Article 101 of the Treaty on the Functioning of the European Union and Article 53 of the EEA Agreement (AT.39914 - Euro Interest Rate Derivatives (EIRD) (Settlement)) (Dec. 4, 2013).

106 See generally Colangelo, *supra* n. 22, at 85-86 (in Google Shopping and LIBOR, marketplace actors relied on the integrity of the process that produced the search results and the benchmark without having the ability to determine its corruption).

Accordingly, whether viewed as coercion of users or corruption of marketplace operations, dark patterns are antithetical to competition on the merits. Market integrity presupposes rational decision-making by informed economic actors — rivals, suppliers, and customers. By surreptitiously manipulating actor decision-making processes, dark patterns undermine market integrity.[107]

These anticompetitive consequences are sufficiently clear that *per se* treatment should apply.[108] Secretly disabling informed and rational user or consumer choice has no redeeming social or economic value.[109] That is the underpinning of not only the denial of First Amendment protection to false or misleading advertising, but also the FCC's position on subliminal advertising. Nothing positive weighs in the balance.[110] To the contrary, failing to recognize the irredeemable quality of dark patterns itself encourages their continued use and expansion to manipulate and exploit online users. Creativity in developing dark patterns, however, is not "innovation" that should be incented.

While these cases do not involve dark patterns, they are instructive nonetheless because they provide an antitrust framework available to plead a claim. One recently filed lawsuit, however, alleges specifically that the defendant, Facebook, used dark patterns for anticompetitive purposes. In *Sherman v. Facebook, Inc.*, the plaintiffs contend that Facebook wrongfully acquired or maintained monopoly power in violation of the Sherman Act, in part, "by deploying dark patterns, skullduggery, and other misleading and fraudulent behavior" in its data collection efforts."[111] According to the plaintiffs, "[d]ark patterns cause consumers to pay a higher data price than they would freely choose. Framing and communication of privacy settings in a way that takes advantage of consumers' behavioral limitations causes them to give away more data and privacy than they otherwise would and represents a lower quality of the service."[112] The court has not yet ruled on the Sherman plaintiffs' claim, however.

X. CONCLUSION

Dark patterns aren't going away. They're getting worse. "[D]esign has been weaponized using behavioral research to serve the aims of the surveillance economy."[113] And as the "internet of things" continues to develop, the opportunities to abuse users and rivals will expand exponentially. Action needs to be taken before dark patterns move from computers, tablets, and mobile phones to heating systems, refrigerators, and all manner of consumer goods.[114]

Seeds of optimism are being planted, however. As the FTC's recent agency workshop and passage of the California Consumer Privacy Act demonstrate, there is now growing interest in fighting back against use of dark patterns. Enforcers, businesses, and consumers should challenge, dark patterns under the antitrust laws, which are well-equipped to tackle this activity. Potential treble damages antitrust liability and attorneys fee recoveries can deter a firm's continuing to resort to dark patterns to exploit users and hinder rivals.

107 See *id.* at 65 ("[T]he idea that consumers select the best firms in the market on the basis of merit does not hold true when consumer opinions are manipulated by false or unduly persuasive information."); Guy Rolnik & Asher Schechter, How Can Antitrust Be Used to Protect Competition in the Digital Marketplace?, Promarket (Sept. 26, 2016) (interview of Ariel Ezrachi: "In the online world, the buyer's rational decision-making is often undermined by a controlled ecosystem in which transparency and choice can be distorted. Perhaps most striking, the targets of these practices — the buyers — are often unaware of the extent of the manipulation."), https://promarket.org/2016/09/26/digital-market-not-going-correct/; Woodcock, *supra* no. 44, at 2276 (footnote omitted) ("Tinkering with the decision-making processes of consumers prevents consumers from rewarding, through their purchase decisions, the innovators who best meet their needs, and thereby threatens the foundation of technological progress in a free market system.") (footnote omitted).

108 Main, *supra* n. 43, at 628-29 ("prohibiting coercive neuromarketing is essential to preserving a fair bargaining process, and therefore, the government could prohibit neuromarketing entirely").

109 See Stigler Center Report, *supra* n. 3, at 238 ("While dark patterns come in a variety of different forms, their central unifying feature is that they are manipulative, rather than persuasive. More specifically, the design choices inherent in dark patterns push users towards specific actions without valid appeals to emotion or reason.").

110 See Main, *supra* n. 43, at 627 ("The same rationale for denying protection to false or misleading speech in advertising also applies to unfairly effective neuromarketing, meaning that the government could constitutionally regulate the use of neuromarketing"). *Cf.* Woodcock, *supra* n. 44, at 2321 (footnote omitted) (persuasive advertising — that which manipulates consumer choice — as opposed to informative or complementary advertising (the former of which provides useful information and the latter of which enhances consumer enjoyment in product use) — should be unlawful *per se* under antitrust principles because, "like price fixing," persuasive advertising is "harmful to consumers in all cases," causing consumers "to pay more for the advertised product for reasons that . . . involve no gain in consumer welfare.").

111 Complaint at ¶79, *Sherman v. Facebook, Inc.*, Docket No. 5:20-cv-08721 (N.D. Cal. Dec 09, 2020).

112 *Id.* at ¶93.

113 Narayanan, *supra* n. 28, at 79.

114 See European Commission, Commission Staff Working Document Preliminary Report - Sector Inquiry into Consumer Internet of Things, SWD(2021) 144 final, ¶ 1.2(3), at 15 (June 9, 2021) ("It is expected that there will be more than 8 billion consumer internet and media devices worldwide by 2030, making this area by far the most common use case of the IoT as a whole") (footnote omitted).

CPI COMPETITION POLICY INTERNATIONAL

CPI Subscriptions

CPI reaches more than 35,000 readers in over 150 countries every day. Our online library houses over 23,000 papers, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.