NOTES

KEEPING CONSUMERS IN THE DARK: ADDRESSING "NAGGING" CONCERNS AND INJURY

*Alison Hung**

In the digital context, companies often use "dishonest design"—commonly known as "dark patterns"—to trick or push consumers into doing things they wouldn't necessarily have done otherwise. Existing scholarship has focused on developing a taxonomy and definitions for different categories of dark patterns, conducting empirical research to better understand the effectiveness of dark patterns, and broadly surveying the legal and regulatory landscape for theories, existing and new, through which to curb these practices. This Note offers a deep dive into one category of dark patterns—"nagging"—and the unique legal issues that the practice raises. While the FTC has started to use its section 5 "unfair or deceptive" authority to combat some other types of dark patterns, particularly practices that mislead consumers, nagging practices are especially elusive—but just as insidious as the more commonly discussed categories of dark patterns. This Note identifies the direct and indirect harms that nagging poses to consumers, argues for the regulation of the nagging category of dark patterns, and proposes a "do not nag" feature, modeled after the federal "do not call" list, as a solution.

* J.D. Candidate 2022, Columbia Law School. The author would like to thank Professor David Pozen for his invaluable guidance and the staff of the *Columbia Law Review* for their thoughtful feedback and excellent editorial assistance. Special thanks to Stephen Ark for his encouragement. All errors are my own.

INTRODUCTION

In 2015, LinkedIn settled for $13 million with users who, after signing up for LinkedIn's "Add Connections" feature, were dismayed to learn that LinkedIn had sent unwanted emails to their address book contacts on their behalf.[1] These LinkedIn users had agreed to send an initial email inviting their professional contacts to connect, but what they didn't know was that LinkedIn would send up to two reminder emails to each contact.[2] Contacts on the receiving end of these reminder emails had virtually no way to opt out of reminders.[3] This is one of the more notorious cases of companies using "dishonest design"—also known as "dark patterns"—to

1. Ahiza Garcia, LinkedIn to Pay $13 Million for Unwanted Emails, Lawyers Could Get $3.3 Million, CNN Money (Oct. 3, 2015), https://money.cnn.com/2015/10/03/news/linkedin-settles-lawsuit-emails/index.html [https://perma.cc/8JNB-BPZC].

2. Id.

3. John Brownlee, After Lawsuit Settlement, LinkedIn's Dishonest Design Is Now a $13 Million Problem, Fast Co. (Oct. 5, 2015), https://www.fastcompany.com/3051906/after-lawsuit-settlement-linkedins-dishonest-design-is-now-a-13-million-problem [https://perma.cc/ZY5T-8XVL].

trick or push consumers into "doing things they don't really want to do."[4] But even though most dark patterns don't make headlines or result in multimillion dollar settlements, they significantly impact consumers' online experiences because they are everywhere.[5]

Many of the basic tactics and strategies underlying dark patterns are neither new nor unique to the online context. Before the advent of the internet, salespeople and marketing professionals had long wielded persuasion, coercion, and even manipulation with great effect.[6] What makes these practices particularly concerning in the digital context, however, is their scale: Online platforms can reach millions of consumers within seconds through targeted advertisements, and companies can use automated tools to spam consumers with marketing emails.[7]

Companies' incentives are not always aligned with consumers' best interests or preferences, and design is a potent tool for companies[8] to shape consumers' digital experiences and influence their behavior.[9] For

---

4. Id.

5. Eric Ravenscraft, How to Spot—and Avoid—Dark Patterns on the Web, WIRED (July 29, 2020), https://www.wired.com/story/how-to-spot-avoid-dark-patterns/ [https://perma.cc/T8R2-B5D3].

6. See Jamie Luguri & Lior Jacob Strahilevitz, Shining a Light on Dark Patterns, 13 J. Legal Analysis 43, 45–46 (2021) (listing door-to-door sales and transactions involving funeral services, telemarketing, and home equity loans as examples of these high-pressure, sometimes questionable sales tactics); see also Fed. Trade Comm'n v. Age of Learning, Inc., No. 2:20-cv-7996, at 1 (C.D. Cal. Sept. 1, 2020) (statement of Comm'r Rohit Chopra, Regarding Dark Patterns in the Matter of Age of Learning, Inc.), https://www.ftc.gov/system/files/documents/public_statements/1579927/172_3086_abcmouse_-_rchopra_statement.pdf [https://perma.cc/V9X5-CWFA] [hereinafter Age of Learning, Statement of FTC Commissioner] (recognizing that dark patterns are "the online successor to decades of dirty dealing in direct mail marketing").

7. Ryan Calo, Digital Market Manipulation, 82 Geo. Wash. L. Rev. 995, 1021 (2014); Justin (Gus) Hurwitz, Designing a Pattern, Darkly, 22 N.C. J.L. & Tech. 57, 67–68 (2020) (suggesting that what is unique about dark patterns is that, in the online context, "[t]here is practically no limit to design choices, and those design choices can be changed, tweaked, updated, and targeted with ease").

8. In the digital context, through A/B testing, companies now have the ability to conduct experiments on consumers to learn how changes in user interface or product design can affect consumers' behavior. See 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/ [https://perma.cc/J2Y9-KJXL] ("A/B [testing] allows seemingly subjective questions of design—color, layout, image selection, text—to become incontrovertible matters of data-driven social science."); Justin Elliott & Paul Kiel, The TurboTax Trap: Inside TurboTax's 20-Year Fight to Stop Americans From Filing Their Taxes for Free, ProPublica (Oct. 17, 2019), https://www.propublica.org/article/inside-turbotax-20-year-fight-to-stop-americans-from-filing-their-taxes-for-free [https://perma.cc/R9YQ-EFVP] (describing how the company "conducts rigorous user testing" to make design choices that "maximize how many customers pay, regardless if they are eligible for the free product," and "[d]ark patterns are something that are spoken of with pride and encouraged" in design meetings).

9. Woodrow Hartzog, Privacy's Blueprint: The Battle to Control the Design of New Technologies 27 (2018) ("Through signals, design helps define our relationships and our

example, companies that mediate consumers' online social interactions have "overwhelming incentives to design technologies in a way that maximizes the collection, use, and disclosure of personal information."[10] Some scholars have argued that design should play a bigger role in privacy law, which has tended to focus more on data collection, use, and distribution.[11] After all, design conveys signals to consumers, affects the transaction costs of their online activities,[12] and affects their perceptions.[13] As Professor Woodrow Hartzog remarks, "Design is everything . . . . [D]esign is power."[14]

Scholarship on dark patterns has focused on developing a taxonomy and definitions for different types of dark patterns, conducting empirical research to better understand the effectiveness of dark patterns, and broadly surveying the legal and regulatory landscape for theories, existing and new, through which to curb these practices—categories of dark patterns ranging from the merely troubling to the clearly manipulative.[15] Scholars and researchers have already identified and recognized "nagging"—online design practices that create persistent interactions with users and may eventually compel them to do things that they wouldn't

---

risk calculus when dealing with others. Design affects our expectations about how things work and the context within which we are acting.").

10. Id. at 5. As Professor Woodrow Hartzog and others have noted, "The predominant Internet business model is built on collecting as much user data as possible and selling it or using it to target and persuade users . . . . Design can be leveraged in subtle ways to get more, more, more." Id.

11. Id. at 12 ("Most students of privacy policy understand privacy by design to mean a proactive ex ante approach to considering and protecting privacy . . . . The opposite of privacy by design is responding to a privacy harm after it has occurred."). The more enforcers overlook design, the more room companies have to use design to run around privacy and other consumer protection laws. See id. at 57 ("Design tricks like manipulative and confusing website design or evasive surveillance devices can be technically legal yet leave people ignorant, deceived, confused, and hurt."); see also Ari Ezra Waldman, Privacy, Notice, and Design, 21 Stan. Tech. L. Rev. 74, 107–08 (2018) (explaining that "users consider design when making privacy choices," not just the substance of privacy policies).

12. See Lauren E. Willis, Why Not Privacy by Default?, 29 Berkeley Tech. L.J. 61, 110–11 (2014) (describing how firms' design and choice-architecture decisions alter or frame the consumer's "decision environment" by affecting transaction barriers).

13. Hartzog, supra note 9, at 42.

14. Id. at 21, 23; see also Calo, supra note 7, at 1004 (noting that a consequence of consumer mediation is that "firms can and do design *every* aspect of the interaction with the consumer" (emphasis added)); Waldman, supra note 11, at 78–79 ("[D]esign configures users, limiting our freedom in ways predetermined by the designer . . . . [W]ebsite design can discourage us from reading privacy notices . . . or coerce us into mismanaging our privacy contrary to our true intentions.").

15. See Luguri & Strahilevitz, supra note 6, at 45 (explaining that existing research focuses on the taxonomy and "growing prevalence of dark pattern techniques"). But see Hurwitz, supra note 7, at 104–05 (arguing that we should first consider existing statutory authority before "overlying new . . . layers to the regulatory fabric," and that the fact that many firms use design for questionable purposes alone "does not demand legislative or regulatory innovation in response . . . [because] the market is an effective check on these practices").

necessarily have done—as one of many categories of dark patterns. This Note contributes to existing legal scholarship by offering a deep dive into the nagging category of dark patterns, particularly the unique legal issues that the practice raises.

This Note argues for the regulation of the nagging category of dark patterns and proposes a "do not nag" feature, modeled after the federal "do not call" list, as a solution. While the FTC has started to use its section 5 "unfair or deceptive" authority to combat some types of dark patterns, particularly practices that mislead consumers, nagging practices are especially elusive—but just as insidious as the more commonly discussed dark patterns. Part I of this Note defines the nagging category of dark patterns and argues that nagging practices are harmful to consumers and warrant timely intervention. In particular, section I.B identifies both the direct and indirect harms that nagging poses to consumers. Part II provides an overview of recent legislative and regulatory responses to dark patterns more generally and explains why existing consumer protection legal frameworks, though likely capable of addressing most other categories of dark patterns, will be ineffective at addressing nagging. Section III.A proposes a "do not nag" feature as a solution to the unique nagging problem, drawing on lessons learned from the "do not call" registry and the (ultimately unsuccessful) "do not track" movement. Section III.B further explores how a "do not nag" feature will survive First Amendment scrutiny and engages with other critiques—that it places too heavy of a burden on consumers and could have unintended consequences—that this solution may face.

I. NAGGING DARK PATTERNS

Dark patterns are "user interfaces whose designers knowingly confuse users, make it difficult for users to express their actual preferences, or manipulate users into taking certain actions."[16] User experience (UX) researcher Harry Brignull first coined the term in 2010 and offered a taxonomy of dark patterns;[17] since then, UX scholars have further refined and expanded Brignull's taxonomy.[18] There are several categories of dark patterns: nagging (repeated requests to do something the company prefers), social proof (false or misleading notices that other customers are making purchases), obstruction (preventing users from canceling or comparison

16. Luguri & Strahilevitz, supra note 6, at 44.

17. Harry Brignull, What Are Dark Patterns?, Dark Patterns, https://darkpatterns.org/index.html [https://perma.cc/AK6Z-EHG2] (last visited Aug. 9, 2021).

18. See, e.g., Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp & Stefan Pfattheicher, Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns, 4 Proc. on Priv. Enhancing Techs. 237, 239 (2016) ("Our framework suggests a list of malicious privacy strategies and psychological aspects for categorizing privacy dark patterns."); Gregory Conti & Edward Sobiesk, Malicious Interface Design: Exploiting the User, *in* Proceedings of the 19th International Conference on World Wide Web 271, 272 (Ass'n for Computing Mach. 2010) (proposing a taxonomy of "malicious interface techniques").

shopping), sneaking (unanticipated automatic subscription renewal, bait and switch), interface interference (aesthetic manipulation, trick questions, preselected defaults, or disguised ads that obscure important information), forced action (consumers are tricked into sharing personal information or registering), scarcity (consumers are led to believe that stock is limited), and urgency (consumers are led to believe that an opportunity is time limited).[19]

This Part describes the nagging category of dark patterns and explains how they hurt consumers. Section I.A offers some examples of nagging and uses the concept of a "nudge" to more specifically define what a nag is. Section I.B argues that nagging is more than a mere annoyance. By enabling firms to bypass consumers' consent and commit "attentional theft," nagging directly hurts consumer welfare. Nagging also causes indirect harms, including making consumers more vulnerable to privacy violations and facilitating firms' anticompetitive conduct.

A. *Defining Nagging*

Nagging dark patterns are repeated interruptions of a user's online interactions, where the user's desired action or task is "interrupted one or more times by other tasks not directly related to the one the user is focusing on."[20] Unlike some other categories of dark patterns, nagging does not rely on deception,[21] nor does it involve manipulation.[22] What is at the crux

---

19. Luguri & Strahilevitz, supra note 6, at 53. In January 2021, consumer advocates asked the FTC to investigate Amazon's process for canceling Prime subscriptions, detailing how "Amazon riddles the process with 'dark patterns' . . . including steps that nestle the choice to leave in between other options to abort the whole process or maintain their membership." Matt Day & Ben Brody, Amazon Makes It Too Hard to Cancel Prime, Groups Tell FTC, Bloomberg (Jan. 14, 2021), https://www.bloomberg.com/news/articles/2021-01-14/amazon-makes-it-too-hard-to-cancel-prime-groups-tell-regulators [https://perma.cc/HWD4-3K25]. Amazon employs the obstruction and interface interference strategies, creating a "roach motel in action: unsubscribing from Amazon Prime takes navigating at least 5 pages, but undoing that choice only takes a single click." Pub. Citizen, Re: You Can Log Out, But You Can Never Leave: How Amazon Manipulates Consumers to Keep Them Subscribed to Amazon Prime (Jan. 14, 2021), https://www.citizen.org/wp-content/uploads/Amazon-Dark-Patterns-FTC-letter-.pdf [https://perma.cc/APW2-UWNB].

20. Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt & Austin L. Toombs, The Dark (Patterns) Side of UX Design, *in* Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems 5 (Ass'n for Computing Mach. Paper No. 534, 2018) (separately paginated work).

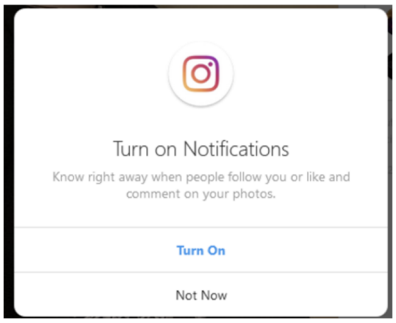
21. See supra text accompanying note 19.

22. This Note adopts the definition of "manipulation" offered by Professors Daniel Susser, Beate Roessler, and Helen Nissenbaum, who characterize manipulative practices as ones that involve influences that are hidden, "exploit cognitive, emotional, or other decision-making vulnerabilities," and are targeted. Daniel Susser, Beate Roessler & Helen Nissenbaum, Online Manipulation: Hidden Influences in a Digital World, 4 Geo. L. Tech. Rev. 1, 27 (2019). An example of online manipulation is behavioral advertising. Id. at 5–6 (describing allegations that Facebook, by monitoring the content and tone of users' posts and interactions, may be able to target teenagers with advertisements during their most vulnerable moments).

of nagging practices is *repetition*—persistence that, whether through persuasion or coercion,[23] can ultimately wear down the consumer into taking the desired action.[24]

1. *Examples of Nagging*. — Nagging is pervasive across digital platforms. Perhaps one of the most well-known examples of nagging is Instagram's repeated pop-ups asking users to turn on their notifications (without giving them a choice to decline):[25]

FIGURE 1: INSTAGRAM POP-UP



In another example, Google prompts users who have disabled "location services" to consider enabling the feature.[26] While this alert does give users the option to actually decline, that choice is not permanent; users will continue to encounter this pop-up each time they open up Google Maps.[27] Over time, users may become so worn down by this unwanted

23. See id. at 15 (drawing a distinction between persuasion and coercion and explaining that "[p]ersuading someone leaves the choice of the matter entirely up to them, while coercing someone robs them of choice . . . although . . . it leaves their capacity for conscious decision-making intact").

24. See Hartzog, supra note 9, at 208 ("We can feel so overwhelmed by the thousands of requests for access, permission, and consent to use our data that we say yes just because we are so worn down."); cf. Omri Ben-Shahar & Carl E. Schneider, The Failure of Mandated Disclosure, 159 U. Pa. L. Rev. 647, 687 (2011) (discussing the "overload problem"—when consumers struggle to comprehend the "avalanche of information" available to them that they often simply do not read the information—as one reason why disclosure mandates often fail to protect personal autonomy).

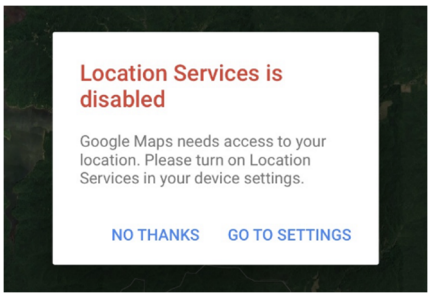
25. Instagram: No Option for "No", UXP^2 Lab: Dark Patterns, https://darkpatterns.uxp2.com/pattern/instagram-no-option-for-no/ [https://perma.cc/9GB5-LV2M] (last visited Aug. 11, 2021).

26. Google Location Services: Spam, UXP^2 Lab: Dark Patterns, https://darkpatterns.uxp2.com/pattern/google-location-services-spam/ [https://perma.cc/5XN3-RG4S] (last visited Aug. 11, 2021).

27. Anthony Bouchard, This Tweak Keeps Google Maps From Nagging You When Location Services Are Disabled, iDB (Nov. 26, 2016), https://www.idownloadblog.com/2016/11/26/google-maps-no-location-services-alert/ [https://perma.cc/5SFH-XVF7]. The Uber app contains another example of nagging: When drivers try to go offline for the day, a pop-up appears, encouraging them to keep driving. Noam Scheiber & Jon Huang, How Uber Uses Psychological Tricks to Push Its Drivers' Buttons, N.Y. Times (Apr. 2, 2017),

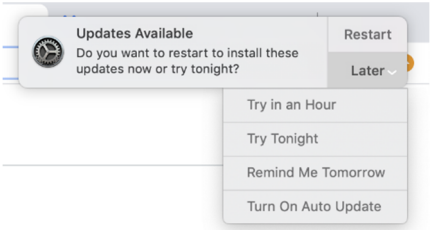
interruption that they simply enable location services to eliminate any future redirection:

FIGURE 2: GOOGLE MAPS POP-UP



To be sure, companies can also mobilize nagging-like strategies to try to nudge users toward taking action that is beneficial.[28] For example, Apple continually prompts its MacBook users to install upgrades, which often include fixes to software bugs and other technical or security issues:[29]

FIGURE 3: MACBOOK SOFTWARE UPDATE



2. *The Blurred Line Between a "Nudge" and a "Nag".* — The concept of a "nudge" may be helpful in describing what nagging is, although distinguishing between the two concepts is often difficult. Professors Richard Thaler and Cass Sunstein developed and proposed the idea of "nudges" as a policy tool—a way for businesses and government to guide people

---

https://www.nytimes.com/interactive/2017/04/02/technology/uber-drivers-psychological-tricks.html (on file with the *Columbia Law Review*).

28. See Richard H. Thaler & Cass R. Sunstein, Nudge: Improving Decisions About Health, Wealth, and Happiness 6 (2008) [hereinafter Thaler & Sunstein, Nudge] (arguing that institutions can help people act beneficially with small changes—"nudges"—in how these institutions structure the choices people face). But see Michal Lavi, Evil Nudges, 21 Vand. J. Ent. & Tech. L. 1, 4 (2018) (describing "evil nudges," which are nudges that negatively influence individual behavior).

29. See What's New in the Updates for macOS Big Sur, Apple, https://support.apple.com/en-us/HT211896 [https://perma.cc/EA7R-8BVP] (last visited Aug. 11, 2021).

toward making choices that would improve their lives.[30] In deciding how to influence the choices other people make, choice architects have a dizzying array of tools at their disposal:[31] They can use defaults to sketch out a path of least resistance,[32] incorporate "error-forgiving innovations" in their designs,[33] and design systems to provide feedback to users.[34] The assumption underlying the notion of a nudge is that public and private actors can use choice architecture to improve outcomes for everyone.[35]

In the digital context, researchers have argued that every design choice is a nudge.[36] And while nudges can guide people toward beneficial behavior, they can also influence people to behave counter to their own interests, particularly when it comes to their online privacy and security.[37] Recognizing the "dichotomous potential" of nudges, researchers have advocated for nudges that steer users "toward decisions that are consistent with their own preferences or objectively improve their welfare."[38]

For the purposes of this Note, "nudges" describe design practices that influence people to take actions or make decisions that align with their own preferences or are beneficial to them. Not all persistent, repeated

---

30. Thaler & Sunstein, Nudge, supra note 28, at 5. The prototypical example of how people can use nudges to influence others' decisions is the arrangement and display of food choices in a school cafeteria. Through arranging how different food choices are displayed—whether to place carrot sticks or french fries at eye level, whether to place desserts first in the line or last—in the cafeteria, a cafeteria worker has considerable influence over what kids choose to eat. Id. at 1–2. Businesses and governments should offer nudges "that are most likely to help and least likely to inflict harm," Thaler and Sunstein argue, especially when people are faced with decisions that are difficult to understand and rare. Id. at 72.

31. A "choice architect" is someone who is tasked with designing the choice environment, including whether and how to nudge people who will have to make a choice at some point. Id. at 73.

32. See id. at 83 ("Defaults are ubiquitous and powerful. They are also unavoidable in the sense that for any node of a choice architecture system, there must be an associated rule that determines what happens to the decision maker if she does nothing.").

33. Id. at 87–88 (explaining that, because humans make mistakes, a well-designed choice system expects users "to err and is as forgiving as possible").

34. See id. at 90 ("Well-designed systems tell people when they are doing well and when they are making mistakes.").

35. See id. at 100 ("[C]hoice architects can improve the outcomes for their Human users.").

36. See Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang & Shomir Wilson, Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online, ACM Computing Survs., at 1, 27 (2017) ("Just as physical design impacts choices, digital design decisions can affect how users behave. Thus, we argue that most User Interface design decisions can be viewed as nudges of some kind.").

37. Id. at 26; see also Waldman, supra note 11, at 79 ("Even seemingly user-friendly design can be manipulative . . . . [P]rivacy policy design, perhaps more than content, has a significant impact on a user's willingness to trust or do business with a website . . . even when user-friendly designs present highly invasive data use practices.").

38. Acquisti et al., supra note 36, at 27.

notifications are created equal. Consider, for instance, notifications that your antivirus protection software is out of date from the antivirus software application on your computer; these notifications don't go away until you update your antivirus software—but that is okay, even desirable, because it is in your best interest to ensure that your computer is shielded from viruses, malware, and spyware. Contrast the antivirus software example with Instagram's recurring pop-ups asking if users want to turn on notifications[39] or an online platform's repeated attempts to get users to consent to tracking via cookie-consent dialogues. These are examples of nagging because they undermine consumers' ability to act according to their preferences and instead promote the best interests of the companies: Obtaining a user's consent for tracking enables firms to collect massive amounts of data on that individual, and influencing a user to turn on notifications can make Instagram's services even more addictive.[40]

In many cases, it is, of course, difficult—if not impossible—to determine what consumers' true preferences are, how they express their preferences, and what actions or decisions would align with these preferences.[41] The distinction between a nag and a nudge is an unstable, dynamic one: What might be an annoying nag to some might be a helpful nudge to others.[42] Thus, any intervention designed to curb nagging should recognize the difficulty, and potential tension, in disentangling consumers' expressed preferences from what would be most beneficial to them.

B. *Nagging's Harm to Consumers*

Nagging has largely evaded the scrutiny placed on some other categories of dark patterns, but nagging practices merit attention because, like other types of dark patterns, they ultimately induce consumers to do or agree to something that they might not have elected or consented to in the practice's absence. Unlike some other types of dark patterns, nagging does not target a specific consumer's vulnerability[43]—instead, nagging

---

39. See supra note 25 and accompanying text.

40. Arvind Narayanan, Arunesh Mathur, Marshini Chetty & Mihir Kshirsagar, Dark Patterns: Past, Present, and Future, 18 ACM Queue 67, 77–78 (2020) (describing dark patterns' three goals as nudging consumers into "spending more than they otherwise would," invading privacy, and making services addictive).

41. See Willis, supra note 12, at 110–11 (discussing how the "very lack of well-formed preferences and a good understanding of the available options . . . leaves consumers vulnerable to firm manipulation").

42. But see Richard H. Thaler & Cass R. Sunstein, Libertarian Paternalism, 93 Am. Econ. Rev. 175, 178–79 (2003) [hereinafter Thaler & Sunstein, Libertarian Paternalism] (critiquing the idea that "people should simply be permitted to choose as they see fit" and defending libertarian paternalism, "an approach that preserves freedom of choice but that authorizes . . . institutions to steer people in directions that will promote their welfare").

43. See generally Shaun B. Spencer, The Problem of Online Manipulation, 2020 U. Ill. L. Rev. 959 (providing background on different types of dark patterns that target specific consumer vulnerabilities); Susser et al., supra note 22, at 12–33 (defining online manipulation and surveying the particular forms it takes).

relies on persistent repetition to wear down consumers. While there is no in-depth empirical analysis focusing on the effectiveness (or perniciousness) of nagging dark patterns in particular yet,[44] Jamie Luguri and Professor Lior Strahilevitz's finding highlighting "the substantial *cumulative* power that different kinds of dark patterns can have" suggests that consumers are especially susceptible to repeated occurrences of dark patterns—similar to how nagging targets consumers through recurrent, persistent interactions.[45] Consumers that ultimately "give in" to nagging probably cannot claim that they didn't understand the transaction to which they agreed or that the company tricked them into consenting. Yet existing scholarship has acknowledged that nagging is problematic in that it compels consumers to do things that they might not have done without the repeated intrusions.[46]

This section builds on this understanding of nagging, taking a deep dive into the various ways in which nagging is harmful. It makes the case that nagging practices are more than a mere annoyance for consumers and that regulators and legislators should take nagging seriously. Specifically, section I.B.1 argues that nagging inflicts direct harms on consumers by rendering their consent meaningless and degrading their online experience through "attentional theft." Section I.B.2 traces nagging's indirect harms and explains how the practice interacts with other features and behaviors of companies to give rise to harms like privacy intrusion and anticompetitive conduct.

1. *Direct Harms: Bypassing Consent and "Attentional Theft".* — Exposing companies' use of nagging dark patterns casts doubt on the validity of the consent obtained from consumers—to having their location tracked, to receiving frequent notifications, or to getting reminders to continue driving for the day. Consumers have started using consent as a basis for challenging dark patterns, though it is unclear whether these challenges will

---

44. Jamie Luguri and Professor Lior Strahilevitz administered an experiment designed to test the efficacy of dark patterns; participants were subject to one of three dark pattern conditions: control group (no dark patterns), mild, and aggressive. To create the dark pattern conditions, Luguri and Strahilevitz employed a *combination* of dark pattern techniques—including nagging as well as other categories of dark patterns, such as roach motels and confusingly worded questions. See Luguri & Strahilevitz, supra note 6, at 58–82. That said, their experiments did not zero in on the effectiveness of the nagging category of dark patterns specifically. More recent research suggests that, unlike some other types of dark patterns, users don't usually detect nagging or become aware that it is functioning as a dark pattern until time has elapsed and the user later experiences an undesired or unnecessary interaction or receives a negative result. Colin M. Gray, Jingle Chen, Shruthi Sai Chivukula & Liyang Qu, End User Accounts of Dark Patterns as Felt Manipulation 17 (Oct. 20, 2020), https://arxiv.org/pdf/2010.11046.pdf [https://perma.cc/C6RM-LEDN] (unpublished manuscript).

45. Luguri & Strahilevitz, supra note 6, at 66 (emphasis added). Further, "[s]ome people who were able to resist certain dark patterns (like roach motels) are still susceptible to falling for others (like confusingly worded questions)." Id.

46. See supra note 40 and accompanying text.

succeed in court.[47] According to Luguri and Strahilevitz, the doctrine of undue influence is "the most promising" legal framework through which consumers can fight dark patterns.[48] While the degree of persuasion necessary to reach the level of unfairness varies based on the circumstances, a consumer seeking to void a contract under the doctrine of undue influence must show that "the result was produced by means that seriously impaired [the consumer's] free and competent exercise of judgment."[49] Applied to nagging practices, however, courts would be reluctant to allow consumers to employ the doctrine of undue influence to undo any contracts to which they assented just to make the nagging stop. Because consumer preferences are so subjective,[50] consumers will struggle to show that, under the objective theory of contract, their externally communicated assent did not reflect their actual preferences.[51]

The European Union General Data Protection Regulation (GDPR) is a prime illustration of consent's central role in regulators' frameworks for protecting consumers from potentially harmful online practices. Under the GDPR, companies must justify personal data collection from consumers on one of six legal bases, one of which is the consent of the data subject—the individual whose data is collected— involved.[52] Moreover, the GDPR defines consent as "any *freely given, specific, informed and unambiguous indication of the data subject's wishes* by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal

---

47. See, e.g., Williams v. Affinion Grp., LLC, 889 F.3d 116, 121–23 (2d. Cir. 2018) (finding that an online shopping company's use of dark patterns did not render void consent to paid membership obtained from consumers, largely because the plaintiffs did not identify any specific representations on the website that were misleading).

48. See Luguri & Strahilevitz, supra note 6, at 94. Undue influence is defined as "unfair persuasion of a party who is under the domination of the person exercising the persuasion or who by virtue of the relation between them is justified in assuming that that person will not act in a manner inconsistent with his welfare." Restatement (Second) of Conts. § 177 (Am. L. Inst. 1981). Furthermore, "[w]here the required domination or relation is present, the contract is voidable if it was induced by any unfair persuasion on the part of the stronger party. The law of undue influence therefore affords protection in situations where the rules on duress and misrepresentation give no relief." Id. cmt. b.

49. Restatement (Second) of Conts. § 177 cmt. b.

50. What may be a nag to one consumer may be a welcome nudge to another. See supra notes 41–42 and accompanying text.

51. See Joshua A.T. Fairfield, Do-Not-Track as Default, 11 Nw. J. Tech. & Intell. Prop. 575, 596–97 (2013) ("[T]he standard for online contracting must be some flavor of objective. Pure subjective preferences are too easy to manipulate . . . . To do otherwise would be to render contracts useless. One party could always claim that she did not truly mean what was in the contract.").

52. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), Recital 40, 2016 O.J. (L 119) 1, 7–8 ("In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law . . . .").

data relating to him or her."[53] In other words, "freely given consent" means that a company must not have "essentially . . . cornered the data subject into agreeing to [it] using their data."[54]

In spite of the significant role that consent plays in consumer protection regulatory frameworks,[55] the widespread use of dark patterns—including nagging—suggests that consent models may sometimes be inadequate in the context of consumer behavior in the digital age. In fact, some commentators have argued that consumer consent on digital platforms has become so distorted and vitiated that many forms of consent obtained online may be inherently tainted or defective.[56] The fact that companies can so effortlessly circumvent the consent problem on digital platforms should raise alarm bells for regulators who have leaned heavily on consent-based regulatory frameworks—especially given the essential role that consent has traditionally played in governing relationships not only between companies and consumers but also between other groups of individuals.[57] At the very least, policymakers should consider when it makes sense to rely on consent and when consent is so compromised that its use becomes pathological.[58]

The harm to consumers who are subject to nagging can be similarly framed in attentional terms—in terms of a degradation of their digital experience. As Professor Tim Wu explains, "Regulators . . . don't have a paradigm for thinking about consumer harms that are not deceptive or involve physical or financial harm, but rather arise from the seizure of attention and consequential cognitive impairments."[59] Wu offers the

---

53. Id. art. 4(11) (emphasis added).

54. Ben Wolford, Proton Technologies AG, What Are the GDPR Consent Requirements?, GDPR.eu, https://gdpr.eu/gdpr-consent-requirements [https://perma.cc/35HL-4C2C] (last visited Aug. 11, 2021).

55. See Neil Richards & Woodrow Hartzog, The Pathologies of Digital Consent, 96 Wash. U. L. Rev. 1461, 1462–63 (2019) ("Consent's power . . . make[s] it an easy legal tool to reach for when we want to regulate behavior . . . . Perhaps nowhere has consent been deployed more frequently as a legal concept than in the context of digital goods and services.").

56. See id. at 1476–91 (outlining three "pathologies of consent" —cases in which consumers in the digital context "consent" to data privacy practices in ways that seem irrational—to illustrate the gap between "gold standard consent" policymakers usually have in mind and consent in practice).

57. See id. at 1462 ("Consent permeates our law. It is one of its most powerful and most important building blocks . . . . It is the basis of contracts, whether for goods, services, real estate, or marriage.").

58. Id. at 1464–65; see also Elizabeth Edenberg & Meg Leta Jones, Analyzing the Legal Roots and Moral Core of Digital Consent, 21 New Media & Soc'y 1804, 1804–05 (2019) ("Valid consent can render permissible an otherwise impermissible action . . . . We can consent to sexual relations, borrowing a car, surgery, and the use of personal information. Without consent, the same actions can become sexual assault, theft, battery, and an invasion of privacy.").

59. Tim Wu, Blind Spot: The Attention Economy and the Law, 82 Antitrust L.J. 771, 778 (2017).

"attentional theft" concept to describe harm to the consumer brought about by nonconsensual and intrusive digital advertising.[60] The same concept could be helpful in describing what precisely is so troubling about nagging, in addition to its implications for consent, privacy, and competition.[61] The example that Wu provides is the problem of phone calls on airplanes: In the face of a growing belief that the traditional rationale for banning cell phone usage on flights—potential interference with traffic control communications—is becoming increasingly obsolete,[62] the Department of Transportation may need to provide an alternative rationale to justify such a ban.[63] Travelers and flight attendants alike, however, expressed concerns about allowing phone calls on flights, citing the "stress, disruption, and rage"—or, to use Wu's term, "attentional intrusions"—that would result if passengers were permitted to take voice calls on airplanes.[64]

Although nags from online platforms do not typically come with the noise that accompanies voice calls involving a hundred people in a small space, the notifications, pop-ups, or intervening webpages negatively impact consumer welfare because they commandeer consumers' attention, a resource that has become all the more precious in the digital age.

2. *Indirect Harms: Privacy Intrusion and Antitrust Implications.* — Nagging can prompt consumers to disclose more personal information or other data than they might otherwise have been comfortable with, providing companies with ever-broadening access to consumer data, such as giving Google Maps permission to track their location at all times,[65] or finally relenting and connecting on LinkedIn.[66] Sharing data with companies could expose consumers to subsequent data breach harms like identity theft or fraud, especially as malicious actors find more efficient, sophisticated ways to exploit consumer data.[67] When it comes to information privacy, consumers are already susceptible to consenting to data policies that they don't fully understand, simply due to the sheer volume of the policies they encounter;[68] nagging further erodes

60. Id.

61. See infra section I.B.2.

62. See Marguerite Reardon, FCC Considers Lifting Cell Phone Ban on Planes, CNET (Nov. 21, 2013), https://www.cnet.com/news/fcc-considers-lifting-cell-phone-ban-on-planes/ [https://perma.cc/7UJT-6Q2P].

63. Wu, supra note 59, at 779.

64. Id. at 778–79. Wu encourages regulators, legislators, and the courts to think about harm to consumers in attentional terms, defining the harm as "the non-consensual seizure of the scarce resource of attention, yielding cognitive impairment." Id. at 780.

65. See supra note 27 and accompanying text.

66. See supra notes 1–3 and accompanying text.

67. See Ido Kilovaty, Legally Cognizable Manipulation, 34 Berkeley Tech. L.J. 449, 451–52 (2019) (describing the proliferation of data breaches and the constantly growing sophistication of hackers and other bad actors).

68. See Commissioner Seeks Public Input on Consent, Off. of the Priv. Comm'r of Can. (May 11, 2016), https://www.priv.gc.ca/en/opc-news/news-and-announcements/2016/

consumers' capacity to reflect on what they're granting permission to companies to do with their data and amplifies the risk of informational harms to consumers.

Potential data breaches and unwitting overdisclosure of information are not the only adverse effects of the lost privacy that results from nagging. Nagging also weakens consumers' ability to negotiate and maintain their boundaries.[69] Courts' discussion of marketing sales calls can be instructive here. When establishing the "do not call" registry to protect consumers from receiving unwanted telemarketing calls, the FCC explicitly noted that the Telephone Consumer Protection Act (TCPA) required the FCC to protect consumer privacy interests.[70] In court, the government has presented its interest in "protecting the privacy of individuals in their homes" as a justification for its "do not call" list.[71] Indeed, the Supreme Court has recognized individuals' privacy interest in "avoiding unwanted communication"—part and parcel of the broader right to be left alone.[72] In *Hill v. Colorado*, the Court emphasized the "enduring importance of 'a right to be free' from persistent 'importunity, following and dogging' after an offer to communicate has been declined."[73] Along those lines, it's not hard to see how nagging is essentially just another form of this "persistent importunity" following a consumer, even after the consumer has already declined the first offer.[74] Many consumers may want to be left alone on their phones and computers, free from recurring, unwanted disruptions to their digital activities,[75] just as consumers thirty years ago wanted to be left alone by relentless telemarketers.

---

an_160511/ [https://perma.cc/X95L-CTPV] (finding that "it would take 244 hours—roughly equivalent to 33 work days—to read all of the privacy policies and related legalese that the average Internet user encounters online each year").

69. See Hartzog, supra note 9, at 71 ("Some adverse effects from lost privacy stem from the inability to negotiate boundaries [and] trust others . . . . When we lose privacy we are forced to watch our back, cover our tracks, and self-censor.").

70. See Rules and Regulations Implementing the Telephone Consumer Protection Act (TCPA) of 1991 ¶ 4, 68 Fed. Reg. 44,144, 44,145 para. 4 (July 25, 2003) ("[I]ndividuals' privacy rights, public safety interests, and commercial freedoms of speech and trade must be balanced in a way that protects the privacy of individuals and permits legitimate telemarketing practices." (internal quotation marks omitted) (quoting In the Matter of the Telephone Consumer Protection Act of 1991, 7 FCC Rcd. 2736, 2744 (1992))).

71. Mainstream Mktg. Servs., Inc. v. Fed. Trade Comm'n, 358 F.3d 1228, 1237 (10th Cir. 2004).

72. Hill v. Colorado, 530 U.S. 703, 716 (2000).

73. Id. at 718 (quoting Am. Steel Foundries v. Tri-City Cent. Trades Council, 257 U.S. 184, 204 (1921)); see also Rowan v. U.S. Post Off. Dep't, 397 U.S. 728, 738 (1970) ("[N]o one has a right to press even 'good' ideas on an unwilling recipient. That we are often 'captives' outside the sanctuary of the home and subject to objectionable speech and other sound does not mean we must be captives everywhere.").

74. In many cases, consumers subject to nagging do not even have the option of truly declining an offer. See supra notes 25–27 and accompanying text.

75. Professor Daniel Solove identified "invasion" as one of four groupings of privacy harms and outlined two types of invasion: intrusion and decisional interference. Daniel J.

Nagging also raises serious antitrust concerns, especially given the influence and prevalence of digital platforms operated by technology companies that have amassed immense market power.[76] Professors Gregory Day and Abbey Stemler argue that dominant technology companies use strategies like dark patterns to exclude competition[77] and generate anticompetitive effects.[78] The same argument applies to nagging. In an age in which a handful of companies dominate digital markets,[79] companies' use of nagging dark patterns is both an indicator and a manifestation of these companies' anticompetitive practices.

Companies with monopoly power may weaponize nagging and use the practice to neutralize competitive threats. In fact, the current dispute between Apple and Tile is an example of how a tech giant (allegedly) used nagging to exclude a potential competitor.[80] Tile, the maker of software and hardware that helps people digitally track the location of their personal belongings, urged the European Commission's antitrust chief to investigate Apple's alleged anticompetitive behavior.[81] Specifically, Tile accused Apple of favoring its own location tracking app, FindMy—recently augmented by a Tile Bluetooth tracking-device equivalent created by

---

Solove, A Taxonomy of Privacy, 154 U. Pa. L. Rev. 477, 552 (2006). Intrusion, Solove argues, "disturbs the victim's daily activities, alters her routines, destroys her solitude, and often makes her feel uncomfortable and uneasy." Id. at 553. Additionally, "[i]ntrusion need not involve spatial incursions: spam, junk mail, junk faxes, and telemarketing are disruptive in a similar way, as they sap people's time and attention and interrupt their activities." Id. at 554.

76. See Majority Staff of H. Subcomm. on Antitrust, Com. & Admin. L. of the Comm. on the Judiciary, 116th Cong., Investigation of Competition in Digital Markets: Majority Staff Report and Recommendations 10–12 (Comm. Print 2020) [hereinafter Majority Staff Report] ("[T]he digital economy has become highly concentrated and prone to monopolization . . . . [D]ominant platforms exploit their gatekeeper power to dictate terms and extract concessions that no one would reasonably consent to in a competitive market.").

77. See Gregory Day & Abbey Stemler, Are Dark Patterns Anticompetitive?, 72 Ala. L. Rev. 1, 35 (2020) (arguing that digital manipulation "can erect barriers to entry where consumers compulsively use a platform to the exclusion of upstarts," excluding competition by "rais[ing] the switching costs of using rival technology").

78. Id. at 36–37 (asserting that dark patterns negatively harm consumers by "extracting wealth from users" and by inducing non-price injuries like quality degradation or reducing consumer choice).

79. See Majority Staff Report, supra note 76, at 11 (noting that companies like Amazon, Apple, Facebook, and Google now dominate and function as "gatekeepers" in certain digital markets, and that in ten years, "30% of the world's gross economic output may lie with these firms" and a few others).

80. See Samuel Axon, iPhone Privacy Prompts Discriminate Against Non-Apple Apps, Complaint Says, Ars Technica (May 29, 2020), https://arstechnica.com/gadgets/2020/05/iphone-privacy-prompts-discriminate-against-non-apple-apps-complaint-says/ [https://perma.cc/2Z2M-26LU]. The author thanks Professor Lina Khan for suggesting this example.

81. Reed Albergotti, Calls Grow for European Regulators to Investigate Apple, Accused of Bullying Smaller Rivals, Wash. Post (May 28, 2020), https://www.washingtonpost.com/technology/2020/05/28/tile-tells-vestager-investigate-apple-antitrust-violations/ (on file with the *Columbia Law Review*) [hereinafter Albergotti, Calls Grow].

Apple called AirTags[82]—by defaulting users to "always allow" location data sharing with FindMy while removing the "always allow" option for the same choice in the competing Tile app when it is newly installed.[83] As a result, Tile argued, Tile and other third-party apps have to repeatedly ask users for permission to turn on the "always allow" location tracking option, which "denigrates the user experience."[84] Even though Tile users could go to "settings" to manually turn on continuous location tracking, third-party apps like Tile would be at a disadvantage in comparison to Apple because "most users stick with the default options in software, rarely going into settings to change options."[85] Continuous location tracking is especially important to technology companies like Tile, whose product functionality would be crippled without always-on location access.[86] Just as news about Apple's efforts underway to create competing hardware (AirTags) leaked,[87] Tile found itself having to nag its users to turn on location tracking, adding frustration to the Tile user experience—frustration that a FindMy/AirTags user would not have to experience.[88] The dispute between Tile and Apple is just one example of how a company with tremendous market power might deploy nagging to edge out competition—all while couching such conduct under the "shield" of

82. J. Fingas, Apple's AirTag Trackers Might Not Arrive Until March 2021, Engadget (Oct. 9, 2020), https://www.engadget.com/apple-airtags-may-be-pushed-to-march-2021-145341210.html [https://perma.cc/P3VF-JJET]; Rebecca Heilweil, Why Apple's Latest Gadget Is Catching the Attention of Antitrust Regulators, Vox: Recode, https://www.vox.com/recode/22395840/apple-airtags-tile-tracker-antitrust-regulators (on file with the *Columbia Law Review*) (last updated Apr. 21, 2021) (describing Tile's concerns that "Apple was making it harder for users to connect their iPhone to Tile devices by requiring permissions . . . that were buried in settings, and prompting users to turn off those permissions after the devices had been set up").

83. Albergotti, Calls Grow, supra note 81.

84. Axon, supra note 80.

85. Reed Albergotti, Apple Says Recent Changes to Operating System Improve User Privacy, but Some Lawmakers See Them as an Effort to Edge Out Its Rivals, Wash. Post (Nov. 26, 2019), https://www.washingtonpost.com/technology/2019/11/26/apple-emphasizes-user-privacy-lawmakers-see-it-an-effort-edge-out-its-rivals/ (on file with the *Columbia Law Review*) [hereinafter Albergotti, Apple Recent Changes].

86. Imran Hussain, Apple Responds to Tile's Complaint to European Commission, Wccftech (May 31, 2020), https://wccftech.com/apple-responds-to-tiles-complaint-to-european-commission/ [https://perma.cc/93LM-KHCK]. Apple defended its actions by pointing to its commitment to user privacy, arguing that this change in users' privacy defaults was made with users' best interests in mind. See Axon, supra note 80. But this user privacy justification is rather tenuous regarding Tile specifically—because users "knowingly buy and use the Tile Bluetooth tracker" for their belongings and therefore "happily provide this [location tracking] data." Imran Hussain, Tile Testifies in Congress Against Apple's iOS 13 Location Tracking Changes, Wccftech (Jan. 19, 2020), https://wccftech.com/tile-testifies-in-congress-against-apples-ios-13-location-tracking-changes/ [https://perma.cc/A7V4-F43N] [hereinafter Hussain, Tile Testifies in Congress].

87. See Hussain, Tile Testifies in Congress, supra note 86.

88. Axon, supra note 80.

privacy.[89] But given the dominance of Apple's App Store and the fact that the company controls "every aspect" of the App Store,[90] Apple could conceivably continue to exploit its control over the App Store ecosystem and selectively use nagging to push consumers away from competing third-party apps.

If Tile's allegations against Apple are true and enforcers are persuaded that Apple is indeed a monopoly, authorities could potentially use nagging to bring a Sherman Act section 2 claim.[91] As applied to the Tile–Apple dispute, nagging could help establish the "exclusionary conduct" requirement of section 2—especially if there is evidence that Apple used nagging as a weapon to neutralize other competitors, not just Tile.[92] From an antitrust perspective, nagging is harmful because companies with monopoly power can leverage the practice to perpetuate their monopoly, thereby chilling competition.[93]

The increasing centralization of digital market power in a handful of platform companies could provide one explanation of why, if nagging

---

89. Albergotti, Apple Recent Changes, supra note 85 (quoting Representative and Chairman of the House Judiciary Antitrust Subcommittee David Cicilline's concern about "the use of privacy as a shield for anti-competitive conduct" and fear that "platforms will exploit their role as de facto private regulators by placing a thumb on the scale in their own favor").

90. Id.

91. The federal antitrust law that is particularly relevant in the nagging dark pattern context is the Sherman Act. Specifically, section 2 of the Sherman Act states: "Every person who shall monopolize, or attempt to monopolize, or combine or conspire with any other person or persons, to monopolize any part of the trade or commerce among the several States, or with foreign nations, shall be deemed guilty of a felony . . . ." 15 U.S.C. § 2 (2018). To prevail on a section 2 claim, the party alleging an antitrust violation must establish two elements: (1) monopoly power in the relevant market, and (2) exclusionary conduct. United States v. Grinnell Corp., 384 U.S. 563, 570–71 (1966) ("The offense of monopoly under . . . the Sherman Act has two elements: (1) the possession of monopoly power in the relevant market and (2) the willful acquisition or maintenance of that power as distinguished from growth . . . as a consequence of a superior product, business acumen, or historic accident."). Furthermore, the exclusionary conduct element requires a showing of an exclusionary act *and* anticompetitive effect. United States v. Microsoft Corp., 253 F.3d 34, 58–59 (D.C. Cir. 2001).

92. In a section 2 claim, it is not enough for the government to show that the monopolist's conduct harmed a *competitor*; the government must establish that the monopolist's conduct harmed *competition*. *Microsoft*, 253 F.3d at 59.

93. Dina Srinivasan has outlined how authorities might bring a section 2 claim under this "leveraging" theory. See Dina Srinivasan, The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy, 16 Berkeley Bus. L.J. 39, 74 n.173 (2019) (discussing how "Facebook's tracking of consumers on third-party sites and leveraging of user IDs may be challenged as illegally maintaining and perpetuating the Facebook monopoly . . . [because] [n]ew entrants . . . that also rely on attracting advertisers cannot compete with Facebook's commercial surveillance"). But see Fed. Trade Comm'n v. Facebook, Inc., No. 20-3590 (JEB), 2021 WL 2643627, at *12 (D.D.C. June 28, 2021) (dismissing the FTC's complaint alleging that Facebook had maintained a monopoly in violation of section 2 because the FTC had failed to establish Facebook's market power).

annoys, inconveniences, and even harms consumers, the market hasn't self-corrected.[94] These online platforms "play an important role in our economy and society as the underlying infrastructure for the exchange of communications, information, and goods and services."[95] For instance, Google currently captures more than eighty percent of the navigation mapping service market through Google Maps,[96] and Apple, through its App Store, controls mobile app access for over 100 million iOS devices across the nation.[97] Consumers often don't flee to a less naggy alternative because, in an economy devoid of genuine competition, there is no viable alternative.[98]

II. ADDRESSING NAGGING: THE FTC'S LIMITED AUTHORITY

While the FTC and consumers likely can use existing legal authority and frameworks to address some categories of dark patterns, nagging will elude regulation. As scholars like Luguri and Strahilevitz have recognized, the legal frameworks for combatting other types of dark patterns—particularly those that are deceptive—largely already exist.[99] For example, some dark pattern techniques, such as the bait and switch, could probably be considered "deceptive" trade practices under the FTC Act.[100] The CFPB

94. See supra notes 76–79 and accompanying text; see also Maximilian Maier & Rikard Harr, Dark Design Patterns: An End-User Perspective, 16 Hum. Tech. 170, 190 (2020) (reporting that respondents to a research study "believed there is no way to avoid dark patterns fully[,] . . . named the dependency on certain services as a reason for that[,] . . . [and thus concluded that] more influential companies can afford to experiment with deceiving techniques without users leaving").

95. Majority Staff Report, supra note 76, at 10.

96. Id. at 15.

97. Id. at 16.

98. See, e.g., id. at 18 ("[T]here is a strong economic incentive for other firms to avoid head-on competition with dominant firms . . . . In the absence of genuine competitive threats, . . . the quality of these services has deteriorated over time . . . . [C]onsumers are forced to either use a service with poor privacy safeguards or forego the service altogether." (footnotes omitted)); Press Release, Letitia James, N.Y. Att'y Gen., Attorney General James Leads Multistate Lawsuit Seeking to End Facebook's Illegal Monopoly (Dec. 9, 2020), https://ag.ny.gov/press-release/2020/attorney-general-james-leads-multistate-lawsuit-seeking-end-facebooks-illegal/ [https://perma.cc/CP3S-WU4S] ("Facebook's unlawful monopoly gives it broad discretion to set the terms for how its users' private information is collected and used to further its business interests . . . . [W]hile consumers initially turned to Facebook . . . seeking privacy protection and control over their data . . . many of those protections are now gone."); see also Alexandra Bruell & Sahil Patel, Facebook's Latest Error Shakes Advertisers' Confidence, Wall St. J. (Nov. 25, 2020), https://www.wsj.com/articles/facebooks-latest-error-shakes-advertisers-confidence-11606346927/ [https://perma.cc/Z773-5D9R] (explaining that, even after Facebook discovered a technical glitch in a tool for advertisers and offered some advertisers millions of dollars in credits, shaking ad buyers' confidence in Facebook's product, marketers "aren't likely to turn away from Facebook").

99. See Luguri & Strahilevitz, supra note 6, at 47.

100. 15 U.S.C. § 45(a) (2018); see also infra section II.A.1.

could combat most dark patterns in the banking and financial services sectors through its authority to regulate "unfair, deceptive, or abusive acts or practices."[101] In other cases, the use of dark patterns could render contractual arrangements void by calling into question consent obtained from a consumer, particularly when consumers unwittingly enter into an agreement that a company presented misleadingly.[102]

But with a category of dark patterns like nagging, it's not so apparent that regulators can as seamlessly use existing laws or legal frameworks to counteract the harms that nagging practices inflict on consumers. After all, nagging, unlike some other categories of dark patterns,[103] does not turn on misleading or manipulating consumers; instead, nagging draws its power from persistence and incessant interruption. This Part outlines why, despite nagging's negative effects on consumers, existing legal frameworks are likely to be inadequate for solving the nagging problem. Section II.A.1 examines how the FTC has begun to address certain categories of dark patterns using its section 5 authority—efforts that are still in their infancy and only address *deceptive* online design practices. Section II.A.2 summarizes the DETOUR Act, Congress's proposed legislation designed to curb dark patterns, which was ultimately unsuccessful but signals regulators' and policymakers' growing awareness of the issue. Section II.B analyzes existing consumer protection laws and explains why attributes specific to nagging dark patterns will nonetheless allow nagging to continue unchecked under the current consumer protection regime, even as policymakers place increased attention on dark patterns generally.

A. *Past and Proposed Regulatory and Legislative Responses to Dark Patterns*

Although the FTC's section 5 "unfair or deceptive" authority could, in theory, allow it to regulate various types of dark patterns, including nagging, the FTC's enforcement actions have primarily focused on curbing deceptive business practices. Dark patterns have also caught the attention of some legislators, who attempted to pass legislation targeting dark patterns in 2019.

1. *The FTC's Section 5 "Unfair or Deceptive" Authority.* — Existing legislative and regulatory enforcement actions have focused on fighting the categories of dark patterns that deceive and mislead consumers, often resulting in clear economic harms. The FTC is empowered under section 5 of the FTC Act to address "unfair or deceptive acts or practices in or affecting commerce."[104] In recent years, the FTC has frequently

101. 12 U.S.C. § 5531 (2018).

102. See supra notes 48–49 and accompanying text.

103. For a discussion of the "sneaking" and "obstruction" categories of dark patterns, see supra text accompanying note 19.

104. 15 U.S.C. § 45(a)(1).

challenged business practices under the deception prong.[105] One of the most notable dark pattern FTC cases is *FTC v. AMG Capital Management, LLC*,[106] which involved a payday lender that employed interface interference tactics to lure customers into opting into terms where they would unknowingly accrue additional finance charges. The Ninth Circuit ultimately agreed with the FTC that the website employed practices that were deceptive.[107]

Also, in September 2020, the FTC settled with Age of Learning, an online children's education company that runs ABCmouse, for $10 million on charges that ABCmouse used dark patterns—specifically, the "roach motel" type of dark pattern to make it extremely difficult for users to cancel recurring subscription fees—to scam millions from families.[108] In a separate statement, then-FTC Commissioner Rohit Chopra explicitly mentioned dark patterns and signaled that the FTC might seek to combat unlawful dark patterns more vigorously in the future.[109]

While the FTC has fought deceptive online design practices, enforcement actions based solely on the unfairness prong have been much more limited. Section 5(n) of the FTC Act codified the three-part test for unfairness, which requires the following elements to establish that a practice is unfair to consumers: (1) The practice causes or is likely to cause "substantial injury" to consumers; (2) that is not "reasonably avoidable" by consumers; and (3) that is "not outweighed by countervailing benefits to consumers or to competition."[110] The FTC will also consider "whether the

105. See, e.g., Fed. Trade Comm'n v. LeadClick Media, LLC, 838 F.3d 158 (2d Cir. 2016) (finding that disguised ads and false testimonials on websites were unlawfully deceptive).

106. 910 F.3d 417 (9th Cir. 2018), vacated, 998 F.3d 987 (mem.) (9th Cir. 2021).

107. The Supreme Court subsequently reversed and remanded: In doing so, the Court did not address whether the business practices involved were deceptive; instead, it focused solely on the issue of whether a different provision of the FTC Act, which authorizes the FTC to obtain a "permanent injunction" in federal court against individuals or organizations who have violated a law that the Commission enforces, also permits the FTC to seek, and a court to award, equitable monetary relief. AMG Cap. Mgmt., LLC v. Fed. Trade Comm'n, 141 S. Ct. 1341, 1344 (2021). The Court concluded that the FTC did not have the statutory authority to obtain equitable monetary relief and reversed the Ninth Circuit's judgment on that ground. Id. at 1352.

108. Complaint for Permanent Injunction and Other Equitable Relief at 3–4, Fed. Trade Comm'n v. Age of Learning, Inc., No. 2:20-cv-7996 (C.D. Cal. Sept. 1, 2020), https://www.ftc.gov/system/files/documents/cases/1723086abcmousecomplaint.pdf [https://perma.cc/S9R5-RUSA]; see also Fed. Trade Comm'n v. Age of Learning, Inc., No. 2:20-cv-7996, at 11 (C.D. Cal. Sept. 8, 2020) (Stipulated Order for Permanent Injunction and Monetary Judgment), https://www.ftc.gov/system/files/documents/cases/1723186abcmouseorder.pdf [https://perma.cc/UWY7-GUYQ].

109. See Age of Learning, Statement of FTC Commissioner, supra note 6, at 3 ("[T]he FTC Act . . . vests the Commission with authority to analyze emerging practices and define which practices are unlawful . . . . [W]e need . . . to shine a light on unlawful digital dark patterns, and we need to contain the spread of this popular, profitable, and problematic business practice.").

110. 15 U.S.C. § 45(n) (2018).

trade practice violates established public policy 'as it has been established by statute, common law, industry practice, or otherwise.'"[111] Although public policy is typically invoked to evaluate whether a consumer injury is substantial, the FTC has indicated that public policy will sometimes independently support an industry action, particularly "when the policy is so clear that it will entirely determine the question of consumer injury, so there is little need for separate analysis by the Commission."[112]

At best, the FTC's use of its unfairness authority has been messy. The FTC has historically avoided invoking its unfairness authority, although recent complaints suggest that the trend is moving in the other direction.[113] Most notably, the Third Circuit held that the FTC has the authority to regulate companies' data security practices under the section 5 unfairness prong,[114] although the vast majority of data security–related administrative actions brought by the FTC have ended in settlement.[115] Scholars have suggested that the FTC should use its unfairness authority much more aggressively to ensure that its consumer protection framework keeps pace with increasingly powerful technology—such as the growing use of predictive analytics, artificial intelligence, and bots[116]—and its rapidly evolving harms, such as manipulation resulting from data breaches.[117] The FTC has also used its unfairness authority to protect consumers from "unfair" retroactive policy changes and "unfair" default settings.[118]

---

111. See Daniel J. Solove & Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 Colum. L. Rev. 583, 639 (2014) (quoting Letter from FTC Comm'rs to Wendell H. Ford & John C. Danforth, Senators, Consumer Subcomm. of S. Comm. on Com., Sci., & Transp. (Dec. 17, 1980), reprinted in In re Int'l Harvester Co., 104 F.T.C. 949, 1070 (1984), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness [https://perma.cc/Z9SK-82EG]).

112. Id. (quoting Letter from FTC Comm'rs to Wendell H. Ford & John C. Danforth, Senators, Consumer Subcomm. of S. Comm. on Com., Sci., & Transp. (Dec. 17, 1980), reprinted in *In re Int'l Harvester Co.*, 104 F.T.C. at 1070).

113. Id. at 638.

114. Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236, 243, 249 (3d Cir. 2015) (finding that Congress designed the FTC's unfairness authority as a "flexible concept with evolving content," and that the FTC could bring unfairness actions against companies engaging in inadequate cybersecurity practices resulting in consumer harm (internal quotation marks omitted) (quoting Fed. Trade Comm'n v. Bunte Bros., 312 U.S. 349, 353 (1941))). But see LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1236 (11th Cir. 2018) (holding that the FTC's cease and desist order against LabMD, who allegedly failed to safeguard consumer data, was unenforceable because it required the company to meet a vague standard of reasonableness, while assuming that the FTC had the authority to regulate cybersecurity).

115. *Wyndham Worldwide Corp.*, 799 F.3d at 240.

116. See, e.g., Terrell McSweeny, Psychographics, Predictive Analytics, Artificial Intelligence, & Bots: Is the FTC Keeping Pace?, 2 Geo. L. Tech. Rev. 514, 525–30 (2018).

117. See Kilovaty, supra note 67, at 497–98.

118. See, e.g., Complaint at 9, In re Facebook, Inc., FTC File No. 0923184, Docket No. C-4365 (F.T.C. Aug. 10, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf [https://perma.cc/SL74-JPM5] (finding that when Facebook applied changes to user profile privacy settings to share personal

2. *The Deceptive Experiences to Online Users Reduction (DETOUR) Act.* — In 2019, Senators Mark Warner and Deb Fischer introduced bipartisan legislation—the Deceptive Experiences to Online Users Reduction Act, or "DETOUR Act"—aimed at curbing dark patterns,[119] but that effort was ultimately unsuccessful. The DETOUR Act sought to prohibit "unfair and deceptive acts and practices relating to the manipulation of user interfaces," making it unlawful for any "large online operator" to, among other things, "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."[120] The Act would have designated the FTC as the enforcement authority and required the Commission to establish a professional standards body to develop further "guidance and bright-line rules for the development and design of technology products of large online operators."[121]

The legislation attracted plenty of skepticism. Some critics feared that the DETOUR Act, in granting "sweeping power" to the FTC, could "make nearly all large web sites presumptively illegal."[122] Others, while recognizing the drafters' efforts to be comprehensive, raised concerns about some vague, abstract wording in the bill: How should enforcers identify a company's "purpose" for designing a user interface?[123] When is the effect of a user interface design "substantial"?[124] Detractors were concerned about the ambiguity in the text of the bill, in both the terms that the Act defined—in abstract language—and the terms that the Act left undefined, ultimately leaving it up to the FTC and to the courts to decide which online practices would be permissible.[125] It is unclear whether legislation like the

---

information that it had previously collected from users, it committed an "unfair act or practice"); Complaint at 3–4, In re Sony BMG Music Ent., FTC File No. 0623019, Docket No. C-4195 (F.T.C. June 28, 2007), https://www.ftc.gov/sites/default/files/documents/cases/2007/06/0623019cmp070629.pdf [https://perma.cc/B45Y-P3L4] (finding that Sony engaged in "unfair acts or practices" when, in selling music CDs to consumers, it did not disclose to customers that presets would cause a proprietary media player on the CD to automatically connect to Internet servers and transmit user information to Sony); In re Gateway Learning Corp., 138 F.T.C. 443, 449 (2004) (complaint) (finding Gateway's practice that retroactively applied a revised privacy policy containing "material changes" to its practices to personal information previously obtained from consumers to be "unfair").

119. Tom McKay, Senators Introduce Bill to Stop 'Dark Patterns' Huge Platforms Use to Trick Users, Gizmodo (Apr. 9, 2019), https://gizmodo.com/senators-introduce-bill-to-stop-dark-patterns-huge-plat-1833929276 (on file with the *Columbia Law Review*).

120. Deceptive Experiences to Online Users Reduction Act, S. 1084, 116th Cong. § 3(a)(1) (2019).

121. See id. § 3(c)–(d).

122. Bhavik Nagda, Dark Patterns and Where to Find Them: The DETOUR Act, Medium (Aug. 13, 2019), https://medium.com/@machinesplussociety/dark-patterns-and-where-to-find-them-the-detour-act-b42ff61e4e17 (on file with the *Columbia Law Review*).

123. Id.

124. See, e.g., id. (expressing concern that the DETOUR Act leaves the task of defining vague terms to judges with little technical expertise).

125. Id.

DETOUR Act would encompass nagging: How can enforcers determine when companies have the "purpose . . . of subverting or impairing user autonomy" in engaging in nagging practices, and does nagging even have the "substantial effect" of impairing user autonomy in the first place?[126]

Given the gridlock that has been prevalent in Congress in the last few years, it is unlikely that there will be a meaningful legislative response to the problem posed by dark patterns in the near future. That said, the fact that such legislation made its way to the Senate in the first place demonstrates that dark patterns and their harmful effects on consumers have caught the attention of lawmakers, and it may not be unrealistic to expect renewed attempts to fight companies' deployment of dark patterns in the medium term.[127] And even if Congress were to pass legislation like the DETOUR Act any time soon, the potential questions and ambiguities facing enforcers and the large online operators who would be subject to the Act would likely overlap substantially with some of the questions that this Note discusses. At the very least, the debates surrounding the DETOUR Act and the feasibility of its implementation reflect some of the most unyielding challenges of addressing the problem of dark patterns—and nagging especially.

B. *The Challenges of Addressing Nagging Through Existing Consumer Protection Laws*

Consumer protection law's limited vocabulary for describing consumer harms and the difficulty of separating minor harms from injuries warranting legal intervention make it difficult for existing laws to curb nagging's harms. While some have suggested that Congress should be wary of developing new legislation in response to dark patterns,[128] this section

---

126. For a discussion of how nagging arguably interferes with consumers' "decisional privacy" and vitiates consent, see supra section I.B.

127. Dark patterns have already made their way into privacy legislation at the state level. In November 2020, California voters approved Proposition 24, the California Privacy Rights Act (CPRA), which modifies the California Consumer Privacy Act (CCPA). Lindsey Tonsager, Libbie Canter, Danielle Kehl & Alexandra Scott, Californians Approve Ballot Initiative Modifying the California Consumer Privacy Act, Covington & Burling LLP: Inside Privacy (Nov. 5, 2020), https://www.insideprivacy.com/ccpa/californians-approve-ballot-initiative-modifying-the-california-consumer-privacy-act/ [https://perma.cc/PGG8-7FW8]. One of the amendments renders consent "obtained through use of dark patterns" invalid, although the definition of dark patterns—"'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'—is unclear and could be the subject of significant debate." Id. (quoting Proposition 24, 2020 Cal. Legis. Serv. Prop. 24 § 1798.140(*l*) (West)). Some of the amendments seem to prohibit nagging, albeit in very specific contexts. For instance, after consumers have opted out of the sale or sharing of personal information, companies must "wait for at least 12 months" before re-requesting authorization. Proposition 24, 2020 Cal. Legis. Serv. Prop. 24 § 1798.135(c)(4).

128. See Hurwitz, supra note 7, at 104–05 (arguing against new legislative or regulatory responses to dark patterns more generally because "almost all of the documented practices

explores the applicability of existing consumer protection laws to nagging and shows why the statutory authority currently in place cannot address the harms caused by nagging.[129]

1. *Limited Definition of "Substantial Injury" Under Section 5 of the FTC Act.* — In exploring how to curb nagging through the FTC's section 5(n) unfairness authority,[130] the biggest hurdle is the provision's "substantial injury" requirement. Any action brought against a company using nagging to coerce consumers will need to allege a specific consumer injury, usually financial.[131] Further, "[a] small degree of harm to a large number of consumers may be deemed substantial, as may a significant risk of harm to each consumer. Emotional harm, other more subjective types of harm, and trivial or merely speculative harm[s] generally would not be considered substantial."[132]

The FTC's and courts' existing conception of consumer harms is too limited. Ultimately, the problem with nagging is that it annoys consumers, degrades their digital experiences, and generally reduces their overall welfare—but these are typically not "harms" that regulators can address through the existing regulatory framework.[133] Wu's concept of attentional theft could be helpful in more concretely elucidating the specific consumer injury that results from nagging.[134] Framing the injury to consumers as one of attentional theft could also serve as a corollary to the privacy intrusion concerns raised by nagging practices,[135] giving authorities a concrete framework with which to protect consumers from a type of harm that

---

that are clearly problematic can also clearly be addressed by the FTC using its existing statutory authority").

129. For a discussion of how nagging harms consumers, see supra section I.B.

130. See supra notes 110–112 and accompanying text.

131. See FTC Policy Statement on Unfairness, FTC (Dec. 17, 1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness [https://perma.cc/FN59-N9ZR] ("In most cases a substantial injury involves monetary harm, as when sellers coerce consumers into purchasing unwanted goods or services . . . .").

132. Michael D. Scott, The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?, 60 Admin. L. Rev. 127, 152 (2008) (cleaned up).

133. The challenge of defining legally cognizable harms in the privacy context is a helpful analogy here. As Hartzog asserts, "When privacy is violated, we inevitably sense that there is a problem but cannot easily articulate a clear, cognizable, and individualized injury. This dissonance between actual privacy harms and those addressed in the law paints us into a corner." Hartzog, supra note 9, at 71. In the privacy context, some scholars have urged the FTC to expand its enforcement efforts beyond identity theft to also consider the "dignity" harms that result from diminished privacy. See, e.g., George Ashenmacher, Indignity: Redefining the Harm Caused by Data Breaches, 51 Wake Forest L. Rev. 1, 49 (2016) ("[T]he FTC should frame the harm in the data breach context—at least where there is no identity theft—as harm to victims' dignity, as opposed to their privacy . . . ."); Day & Stemler, supra note 77, at 40 ("Recognizing the panoply of methods used to extract data and attention where few consumers would suspect it, the FTC should expand privacy enforcement beyond mere identity theft.").

134. For a discussion of attentional theft, see supra notes 59–64 and accompanying text.

135. See supra section I.B.2.

to date has escaped meaningful regulation, in large part because it does not fit neatly into the physical harm, financial loss, or deception categories of consumer injury. Until the FTC and courts recognize attentional theft as a consumer injury that warrants intervention, however, most cases of nagging will evade regulation, unless they interact with companies' other practices to produce harms that *are* already legally cognizable, such as some privacy harms.[136]

2. Nagging as an "Abusive" Practice. — Some scholars have called on Congress to expand the FTC's section 5 authority to prohibit "abusive" trade practices in addition to deceptive and unfair practices, recognizing that dark patterns "are often not outright deceptive nor do they necessarily cause the significant kind of harm contemplated by unfairness rules."[137] The CFPB already has the authority to regulate "abusive conduct," though the CFPB's authority is limited to the banking and financial sectors.[138] Under 12 U.S.C. § 5531, an act or practice is "abusive" if it: (1) "materially interferes with the ability of a consumer to understand a term or condition of a consumer financial product or service," or (2) "takes unreasonable advantage of" the consumer's lack of understanding of the "material risks, costs, or conditions of the product or service," inability to protect her own interests in selecting or using a product or service, or "reasonable reliance" on a person covered under the statute to "act in the interests of the consumer."[139] As Hartzog has recognized, lawmakers could transplant this notion of abuse to "shore up some of the limitations of regulating deceptive design, which relies upon untrue signals or broken promises."[140] He argues that the law should address designs "that take unreasonable advantage of people's understanding, limited abilities, or reliance on relationships and transaction costs."[141]

---

136. See supra notes 65–75 and accompanying text; see also Julie E. Cohen, Between Truth and Power: The Legal Constructions of Information Capitalism 56 (2019) (explaining how the FTC attempted to use its section 5 authority to "fill the regulatory gap" for addressing "surreptitious tracking and 'behavioral advertising,'" which, in practice, elevated notice and consent as the "dominant regulatory framework" and privacy policies as "the de facto vehicle for ensuring compliance").

137. Chris Jay Hoofnagle, Woodrow Hartzog & Daniel J. Solove, The FTC Can Rise to the Privacy Challenge, but Not Without Help from Congress, Brookings (Aug. 8, 2019), https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/ [https://perma.cc/MM6M-XGBG].

138. See Luguri & Strahilevitz, supra note 6, at 91; see also Hartzog, supra note 9, at 144 (borrowing from the notion of abusive acts in the Dodd–Frank Wall Street Reform and Consumer Protection Act to "argue that privacy law should seek to recognize and limit abusive design").

139. 12 U.S.C. § 5531(d)(1)–(2) (2018).

140. Hartzog, supra note 9, at 144–45 ("Abusive design overlaps with deceptive and dangerous design, but it is unique. Deception largely deals with problems of false or imperfect information . . . . Abusive design has a different focus. It looks to the problems people have in assessing risk and benefits *even with accurate, truthful information*." (emphasis added)).

141. Id. at 145.

Nagging could fall into the category of an "abusive" design practice—after all, it is usually not deceptive and would most likely fail to meet the unfairness requirements.[142] For instance, a consumer who is faced with a request to turn on location services for the tenth time and finally acquiesces to make the pop-up disappear likely has not fully weighed the "material risks, costs, or conditions" of doing so.[143] Alternatively, a consumer who turns on location services could do so having reasonably relied on the belief that the company would act in her best interests. Deceptive design "misrepresents reality and subverts expectations," whereas "abusive design uses our own internal limitations against us."[144] People's brains have a limited capacity to process information and assess risks,[145] and nagging arguably capitalizes on the limits of human cognition and willpower to prompt consumers to act in line with the company's interests, rather than their own best interests.

3. *The Line-Drawing Problem.* — The line-drawing problem regarding nagging is especially challenging: Getting the same app or website notification once or twice does not seem bad at all, but at what point do repeated interactions become enough of a nuisance to be harmful to consumers? Not every repeat communication qualifies as nagging. Companies, even before the advent of online technology, have long employed aggressive sales and marketing tactics in an effort to appeal to and persuade consumers.[146] In fact, every digital user interface design choice affects how consumers behave and understand the information presented to them.[147] The majority of design choices are harmless and even necessary,[148] but sometimes "the design of information technologies crosses the line and becomes abusive. It unreasonably frustrates our ability to make autonomous decisions and puts us at greater risk of harm or makes us regret our decisions."[149] Most people will agree that some design practices are impermissible, but the tough question is: When does a practice cross the line?[150]

---

142. See supra section II.B.1.

143. Hartzog, supra note 9, at 144.

144. Id. at 143.

145. See Christine Jolls, Cass R. Sunstein & Richard Thaler, A Behavioral Approach to Law and Economics, 50 Stan. L. Rev. 1471, 1477 (1998) ("Bounded rationality . . . refers to the obvious fact that human cognitive abilities are not infinite.").

146. As Hartzog recognizes, "We have a word for communication meant to persuade us to use a product or service: *advertising*." Hartzog, supra note 9, at 143.

147. See supra note 36 and accompanying text.

148. Some would argue that sometimes it is impossible to avoid choice architecture or even default rules and settings. See Hurwitz, supra note 7, at 69 ("[N]ot all 'dark' patterns are intentional or malicious . . . . Design decisions are necessary to any interface and negative effects may be inadvertent or practically unavoidable.").

149. Hartzog, supra note 9, at 143.

150. Luguri & Strahilevitz, supra note 6, at 97 ("[M]ost readers will have some sympathy for the idea that dark patterns could be so pervasive . . . as to obviate consent. But the hard question . . . is 'where does one draw the line?'").

Consider, for instance, how regulators would determine which nagging practices constitute "abusive conduct" and which do not (assuming that the FTC did have the authority to address abusive practices on top of its existing deception and unfairness jurisdiction).[151] For example, when does nagging take "*unreasonable* advantage" of consumers' lack of understanding of what they're signing up for?[152] And, for that matter, is it ever reasonable for companies to engage in practices that take advantage of consumers in that way? While enforcers and the courts will likely always have—and should have—some amount of discretion in making these judgments, guidelines or standards are necessary to constrain that discretion.[153]

The difficulty of determining when repeated interactions rise to the level of nagging, as well as the imprecision of the distinction between a consumer-welfare-enhancing nudge and a consumer-welfare-reducing nag,[154] however, suggest that a top-down, categorical response to nagging would be ineffective. Even as researchers' and regulators' understanding of dark patterns continues to grow, an approach in which a government regulator defines which types of practices are permissible and which are not, while potentially suitable for other categories of dark patterns, would fail to address nagging; after all, individual consumers may have differing views on whether a repeated interaction is harmful. For these reasons, a more consumer-driven, decentralized solution to the problem of nagging would be most likely to succeed.

III. "DO NOT NAG"

Regulators have already signaled that they may begin to more closely scrutinize dark patterns and their impact on consumers.[155] Although the FTC might be able to combat certain categories of dark patterns under its current section 5 authority,[156] nagging does not fit neatly into the FTC's deception and unfairness jurisdiction.[157] Nagging's harms to consumers—such as attentional theft[158]—are not legally cognizable injuries, at least when viewed in light of the section 5 unfairness doctrine's "substantial

151. See supra section II.B.2.

152. 12 U.S.C. § 5531(d)(2) (2018) (emphasis added).

153. See Hartzog, supra note 9, at 148 ("[Dark patterns] are common. Often they are only mildly annoying . . . . Yet in context and in combination with each other, many should be seen as unreasonably abusive. Drawing the boundaries for abusive design will be very difficult because they need to be sensitive to context yet clear enough to follow.").

154. See supra notes 41–42 and accompanying text.

155. See Age of Learning, Statement of FTC Commissioner, supra note 6, at 3 ("If the Federal Trade Commission aspires to be a credible watchdog of digital markets, the agency must . . . go after large firms that make millions, or even billions, through tricking and trapping users through dark patterns.").

156. See supra section II.A.1.

157. See supra note 132 and accompanying text.

158. See supra section I.B.1.

injury" requirement.[159] And yet nagging practices continue to frustrate consumers and undermine their autonomous decisionmaking in their interactions with companies.[160] As then-Commissioner Chopra wrote, "We cannot replicate the whack-a-mole strategy that we have pursued on pressing issues like fake reviews, digital disinformation, and data protection."[161] Legislation like the DETOUR Act would be a step in the right direction, but even that kind of legislation might fail to address nagging.[162] Part III proposes a "do not nag" feature as a solution to the nagging problem that will balance consumer interests and companies' interest in communicating freely with their customers. Section III.A traces the development of the federal "do not call" registry, the inspiration for the proposed solution, then moves to a discussion of the conversation around a potential "do not track" solution, and concludes with a proposal of what an effective "do not nag" scheme could look like. Section III.B addresses potential challenges that "do not nag" may face and explains why concerns that "do not nag" would violate the First Amendment, overburden consumers, or have unintended negative impacts on consumer welfare are misplaced.

A. *Telemarketing Regulations: A Model for a Solution to Nagging*

The national "do not call" registry is a successful solution to the proliferation of unwanted telemarketing calls, a problem analogous to nagging, which consists of firms' unwelcome, repeated digital communications with consumers. This section explores the design and implementation of the "do not call" registry, with a focus on the features that have made it successful, and contrasts it with the failed attempt at establishing a "do not track" feature. This section concludes with a proposal of a "do not nag" feature as a solution to the nagging problem.

1. *The National "Do Not Call" Registry.* — Nagging practices are not new or unique to the online context; telemarketing calls, for example, are a physical-world equivalent, and unwanted sales calls have long been recognized as privacy intrusions.[163] Regulators implemented the national "do not call" registry in response to the proliferation of unwanted sales calls.[164]

---

159. See supra section II.B.1.

160. See Age of Learning, Statement of FTC Commissioner, supra note 6, at 2 (explaining that "[d]ark patterns exist across the internet" and seek "to frustrate users").

161. Id. at 3. In April 2021, the FTC hosted "Bringing Dark Patterns to Light: An FTC Workshop," which "brought together researchers, legal experts, consumer advocates, and industry professionals to examine what dark patterns are and how they affect consumers and the marketplace." Bringing Dark Patterns to Light: An FTC Workshop, FTC: Protecting America's Consumers (Apr. 29, 2021), https://www.ftc.gov/news-events/events-calendar/bringing-dark-patterns-light-ftc-workshop [https://perma.cc/C79E-GMRG].

162. See supra section II.A.2.

163. See Luguri & Strahilevitz, supra note 6, at 46.

164. National Do Not Call Registry FAQs, FTC: Consumer Information, https://www.consumer.ftc.gov/articles/national-do-not-call-registry-faqs [https://perma.cc/KA98-UKF3] [hereinafter National Do Not Call Registry] (last updated May 2021).

In fact, nagging and similar practices arguably carry a greater potential of harm in the online context, given the online ecosystem's unprecedented scale and reach.[165]

The national "do not call" registry, which is managed by the FTC and went into effect in 2003, enables consumers to opt out of unwanted sales calls.[166] Consumers can register their home or mobile phone numbers at no charge with the FTC.[167] It is illegal for businesses to initiate any outbound sales calls to consumers whose telephone number is on the "do not call" list.[168] The "do not call" list applies to "any plan, program or campaign to sell goods or services through interstate phone calls."[169] Sellers, telemarketers, and other service providers are required to access the registry and update their call lists by checking the registry at least every thirty-one days.[170] The registry only prohibits sales calls; political calls, charitable calls, debt collection calls, informational calls, and telephone surveys are allowed—as long as these calls don't also include a sales pitch.[171] If a consumer has recently done business with a company or given a company written permission to call, the company can call with a sales pitch, but the company must stop if the consumer subsequently asks it to.[172] In 2009, responding to developments in technology and sellers' ever-evolving tactics to reach consumers, new rules prohibiting robocalls went into effect.[173] The FTC is responsible for enforcing the "do not call" registry and is authorized to collect annual fees in order to implement the regulatory scheme.[174] Failure to comply could result in fines of over $43,000 per violation.[175] That said, the FTC does not actually block calls from businesses to consumers, so some telemarketers may choose to ignore the registry and continue (illegally) calling consumers on the list.[176] Consumers are

165. See supra notes 6–7 and accompanying text.

166. See 15 U.S.C. § 6151(a) (2018) ("The Federal Trade Commission is authorized under section 6102(a)(3)(A) of this title to implement and enforce a national do-not-call registry.").

167. See National Do Not Call Registry, supra note 164.

168. 15 U.S.C. § 6151(a).

169. Q&A for Telemarketers & Sellers About DNC Provisions in TSR, FTC: Protecting America's Consumers (Aug. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/qa-telemarketers-sellers-about-dnc-provisions-tsr [https://perma.cc/FWF6-Y69X] [hereinafter Q&A for Telemarketers].

170. Id.

171. See National Do Not Call Registry, supra note 164.

172. Id.

173. See Robocalls: Robocalls and the Do Not Call Registry, FTC: Protecting America's Consumers, https://www.ftc.gov/news-events/media-resources/do-not-call-registry/robocalls [https://perma.cc/94EK-R9XG] (last visited Aug. 11, 2021).

174. 15 U.S.C. § 6152(a) (2018) ("The Federal Trade Commission shall assess and collect an annual fee pursuant to this section in order to implement and enforce the 'do-not-call' registry as provided for in section 310.4(b)(1)(iii) of title 16, Code of Federal Regulations . . . .").

175. Q&A for Telemarketers, supra note 169.

176. National Do Not Call Registry, supra note 164.

encouraged to report unwanted calls to the FTC at www.donotcall.gov; the FTC analyzes these reports to identify and impose fines on businesses that place illegal sales calls.[177]

The "do not call" registry has been "extremely popular" with consumers, who previously had little recourse to address the unwanted intrusions.[178] In part, consumers have embraced the registry due to the ease with which it enables consumers to opt out of telemarketing.[179] A key feature of the "do not call" registry and similar privacy regulations is that they "do not make choices for consumers. Instead, they *enable* choices."[180]

2. *"Do Not Track".* — Relatedly, in 2010, the FTC considered implementing a "do not track" mechanism to protect consumers from online advertisers that collect behavior-based data to serve targeted ads, drawing inspiration from the "do not call" registry.[181] Consumers balked at the realization that big technology companies were tracking their online browsing activity across sites to serve up targeted advertisements, and the idea of "do not track" was born.[182] The concept was simple: Consumers could check a box in their browser settings, thus opting out of tracking; it was a "great idea" because checking the box merely meant that consumers were opting out of the tracking technology, not from advertising altogether.[183] The ad tech industry, government, and privacy groups formed a working group to determine how to operationalize "do not track," seemingly "preempting the need for regulation."[184] The idea soon fizzled out,

177. See id.

178. Chris Jay Hoofnagle, Ashkan Soltani, Nathaniel Good, Dietrich J. Wambach & Mika D. Ayenson, Behavioral Advertising: The Offer You Cannot Refuse, 6 Harv. L. & Pol'y Rev. 273, 290 (2012); see also Willis, supra note 12, at 108 ("Despite having to take some action to opt into the list, consumers placed ten million phone numbers on it in the first four days it was operative, and today over seventy percent of Americans have placed their numbers on the list."). But see Glenn Fleishman, How the Tragic Death of Do Not Track Ruined the Web for Everyone, Fast Co. (Mar. 17, 2019), https://www.fastcompany.com/90308068/how-the-tragic-death-of-do-not-track-ruined-the-web-for-everyone/ [https://perma.cc/22KZ-3P5S] ("Do Not Call was ultimately a failure, because it only prevented scrupulous parties from calling, not those who blithely ignored the law or were engaged in outright scams.").

179. Hoofnagle et al., supra note 178, at 290 ("[T]he Telemarketing Do Not Call Registry . . . enables consumers to easily opt out of telemarketing. Prior to the creation of the extremely popular Registry, consumers had few effective tools to address telemarketing intrusions.").

180. Id. (emphasis added).

181. Kenneth Corbin, FTC Mulls Browser-Based Block for Online Ads, Internet News (July 28, 2010), https://www.internetnews.com/it-management/ftc-mulls-browser-based-block-for-online-ads/ [https://perma.cc/DG9R-EEYH].

182. See Fleishman, supra note 178 ("[P]eople were . . . irate about ad networks that followed their activity across sites in order ever more precisely to target marketing messages. A feature called Do Not Track arose as a simple, comprehensible way for browser users to take back their privacy.").

183. Id.

184. Id.

however, because the government, ad tech providers, and browser companies couldn't reach a consensus on how to implement "do not track" as a fully formed regulatory requirement,[185] and browser companies took matters into their own hands. In 2012, for example, Microsoft preset Internet Explorer's "do not track," turning it on for users by default.[186] Google Chrome, Mozilla Firefox, and Apple Safari followed suit and added "do not track" options for users.[187] To make matters worse, the vast majority of websites disregarded "do not track," even for consumers who had turned on the feature in their browser settings.[188] One of the biggest problems with "do not track" was that, unlike the "do not call" registry, it was a standard without any teeth: Companies faced no consequences for ignoring it.[189]

In 2019, "do not track" appeared to be poised for a comeback. Gabriel Weinberg, the CEO of internet privacy company (and search engine) DuckDuckGo, developed a draft bill "aimed at giving the Do Not Track standard a legal force it's never had before."[190] Contemporaneously, Senator Josh Hawley introduced the Do Not Track Act, which would "create a national list that would provide people with an option to block any secondary data tracking and penalize companies that continued to collect unnecessary data."[191] Under the proposed legislation, the FTC would be responsible for enforcing "do not track," and companies violating "do not track" would be subject to a penalty not less than $100,000 and could be fined up to $1,000 a day per person.[192] While these efforts ended up being unsuccessful, the surprise reemergence of "do not track" in recent discussions about protecting consumer privacy demonstrates the continuing promise of consumer protection regimes similar to the "do not call" registry.

3. *Implementing "Do Not Nag".* — A potential solution to nagging would be a "do not nag" mechanism for consumers to opt out of repeated notifications or intrusions from companies, whether on their web browsers

185. Id. (noting that a working group composed of industry and government representatives failed to reach an agreement on how to implement "do not track" regulation).

186. Id.

187. Chris Hoffman, RIP "Do Not Track," the Privacy Standard Everyone Ignored, How-To Geek (Feb. 7, 2019), https://www.howtogeek.com/fyi/rip-do-not-track-the-privacy-standard-everyone-ignored/ [https://perma.cc/RTF2-KKJ4].

188. Id. ("The vast, vast majority of websites ignored ["do not track"]. That never really changed. There was no penalty for ignoring the request and little reason to actually honor it.").

189. Id.

190. Russell Brandom, DuckDuckGo Wrote a Bill to Stop Advertisers From Tracking You Online, Verge (May 1, 2019), https://www.theverge.com/2019/5/1/18525140/do-not-track-duckduckgo-ad-tracking/ [https://perma.cc/N55C-WR4P].

191. Makena Kelly, Senator Proposes Strict Do Not Track Rules in New Bill, Verge (May 20, 2019), https://www.theverge.com/2019/5/20/18632363/sen-hawley-do-not-track-targeted-ads-duckduckgo/ [https://perma.cc/3GFK-VLAR].

192. Do Not Track Act, S. 1578, 116th Cong. (2019).

or mobile devices. Drawing from lessons learned from the implementation of the "do not call" registry and the failed attempts to establish a "do not track" list, a "do not nag" feature needs to have the following characteristics in order to be effective: (1) It must clearly define what it will—and will not—do; (2) it should be backed by the force of legislation, with accompanying penalties for companies who continue to nag consumers; and (3) it should clearly assign enforcement responsibility, likely to the FTC.

Like the "do not call" registry, a "do not nag" feature should enable choices for consumers, not make choices for them. Consumers would be able to opt into "do not nag" by making a selection in their browser, device, or app settings. Withholding the option from consumers to decline a request or say "no" outright—in other words, to stop the nagging—is a common feature of nagging practices. The "do not nag" mechanism could take the form of guidelines for companies' choice architecture,[193] including requiring companies to explicitly provide consumers who have opted not to be nagged with the straightforward option to decline a request once and for all—or at least until a new or improved feature, product, or service offering becomes available. Therefore, a company's digital interaction with a consumer who has opted into "do not nag" would look different from that company's communication with a consumer who has not made the same choice: The former would see "yes," "not now," *and* "no" options, whereas the latter might only see the "yes" and "not now" options (assuming the company still wants to deploy nagging practices where possible). A consumer who has told a company "no" should not receive the same request or communication again. Consumers who have opted into "do not nag" but still encounter nagging practices should be able to report those violations through a www.donotnag.gov website.

To ensure that "do not nag" does not follow the same ill-fated path as "do not track", Congress would need to pass legislation giving the regulatory scheme legal force and subjecting companies that ignore consumers' "do not nag" preferences to significant penalties.[194] Similar to the "do not call" list, companies could face fines capped at a specific dollar amount

193. Choice architecture is the practice of influencing choice by "organizing the context in which people make decisions." Richard H. Thaler, Cass R. Sunstein & John P. Balz, Choice Architecture, *in* The Behavioral Foundations of Public Policy 428, 428 (Eldar Shafir ed., 2013).

194. Although the FTC technically has existing authority under section 5 to promulgate rules, such regulations must adhere to the Magnuson–Moss procedures, which are lengthy and complex; the process includes providing congressional committees and the public with an advance notice of proposed rulemaking, as well as oral hearings before an independent hearing officer, if requested. In fact, the FTC has not promulgated rules under these procedures since 1980. U.S. Gov't Accountability Off., GAO-19-427T, Internet Privacy: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility 12 (2019). Instead, the FTC has, with explicit statutory authorization from Congress, issued regulations subject to the requirements of the Administrative Procedure Act. Id.

per violation.[195] And like the "do not call" registry, "do not nag" could include a "safe harbor" for inadvertent mistakes.[196] Additionally, this legislation should delegate the authority—and obligation—to administer "do not nag" to a government agency with expertise in consumer protection, such as the FTC. Lessons learned from the "do not call" registry and the failed "do not track" initiative indicate that *who* is tasked with implementing and enforcing the opt-out scheme matters as much as what the opt-out scheme itself looks like. When the party shaping the opt-out process and presenting the opt-out to the consumer has "a strong interest in pushing consumers in or out of the default," the opt-out regime is less likely to succeed because the party can use its access to "powerfully influence the consumer's ultimate position."[197] The FTC, unlike telemarketers, does not have a strong reason to prefer that consumers opt into the "do not call" registry or forgo the option;[198] thus, the consumers "who do not sign up have the least to gain by doing so, . . . [while] those who have much to gain sign up."[199]

B. *Potential Challenges to "Do Not Nag"*

A solution like "do not nag" could face challenges from critics asserting that the solution would violate the First Amendment and place additional burdens on consumers, who already face an overwhelming avalanche of information and choices in the digital environment. Moreover, policymakers should consider whether a "do not nag" feature could inadvertently open the door to new, unanticipated consumer harms, especially if firms feel compelled to turn to other kinds of unfair or deceptive business practices.

1. *First Amendment Considerations.* — As Luguri and Strahilevitz note, "Nagging presents perhaps the thorniest type of dark pattern from a First Amendment perspective."[200] Indeed, the issue of whether "unfair" or "abusive" but not deceptive commercial speech is protected under the First Amendment presents one of the biggest obstacles to regulation of the

---

195. In the "do not nag" context, a violation could be defined as each repeated digital communication or interaction.

196. The Telemarketing Sales Rule includes a "safe harbor" provision, which allows a telemarketer to avoid penalties or sanctions if it can establish that the call was made in error and that it followed certain registry procedures and best practices. Complying with the Telemarketing Sales Rule, FTC: Protecting America's Consumers (June 2016), https://www.ftc.gov/tips-advice/business-center/guidance/complying-telemarketing-sales-rule#registry/ [https://perma.cc/WDP5-LD3D] (last updated Jan. 2021).

197. Willis, supra note 12, at 110.

198. See id. at 109–10 (contrasting the successful "do not call" default scheme with financial information and overdraft defaults, where the latter are implemented by financial institutions that profit from sharing customer information with third parties and charging overdraft fees and therefore want consumers to retain their default settings).

199. Id. at 108.

200. Luguri & Strahilevitz, supra note 6, at 100.

nagging problem. Companies might challenge federal law rolling out a "do not nag" mechanism under the First Amendment and argue that requiring companies to adhere to guidelines for choice architecture constitutes an impermissible restriction on commercial speech.

To determine when restrictions on commercial speech run afoul of the First Amendment, courts apply the four-part test laid out in *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*.[201] Under the *Central Hudson* test, a court conducts a four-step analysis: (1) Does the "speech" concern lawful activity, and is it misleading? (2) Is the asserted governmental interest substantial? (3) Does the regulation directly advance the governmental interest asserted? and (4) Is the regulation more extensive than necessary to serve that interest?[202] Under existing legal frameworks, nagging is neither misleading nor unlawful,[203] so it will likely be considered commercial speech.[204] That said, courts will probably recognize the government's substantial interest in safeguarding consumer privacy and protecting consumers from "abusive" design practices like nagging,[205] and that implementing a "do not nag" feature directly advances this interest.

Regarding the fourth *Central Hudson* factor, a court would likely find that "do not nag" is not more extensive than necessary to serve the government's interest in protecting consumers from harmful design practices. In the face of First Amendment challenges, courts have repeatedly upheld the national "do not call" registry as constitutional.[206] Specifically, the Tenth Circuit cited "four key aspects" of the "do not call" registry—that the registry only restricted sales calls instead of all calls from telemarketers, that the registry "targets speech that invades the privacy of the

---

201. 447 U.S. 557 (1980) (holding that a New York Public Service Commission regulation that completely banned promotional advertising by an electrical utility was unconstitutional).

202. Id. at 566.

203. See supra section II.B.1.

204. As Professors Jeremy Kessler and David Pozen note, "[O]ur relatively recent passage from a predominantly industrial to a predominantly informational economy . . . make[s] it increasingly difficult to separate economic activity from expressive activity." Jeremy K. Kessler & David E. Pozen, The Search for an Egalitarian First Amendment, 118 Colum. L. Rev. 1953, 1971–72 (2018). In the digital age, the "communicative dimension" of economic activity has become increasingly pronounced and the creation and circulation of information more central than ever. Id. at 1972.

205. Cf. Mainstream Mktg. Servs., Inc. v. Fed. Trade Comm'n, 358 F.3d 1228, 1232–33 (10th Cir. 2004) (recognizing "the government's important interests in safeguarding personal privacy and reducing the danger of telemarketing abuse" in upholding the "do not call" registry).

206. See, e.g., Nat'l Fed'n of the Blind v. Fed. Trade Comm'n, 420 F.3d 331, 351 (4th Cir. 2005) ("Our Constitution does not prevent the democratic process from affording the American family some small respite and sense of surcease. . . . [W]e find that the [Telemarketing Sales Rule] is consistent with the First Amendment."); *Mainstream Mktg. Servs.*, 358 F.3d at 1250–51 (holding that the "do not call" registry is a valid commercial speech regulation under the *Central Hudson* test).

home, a personal sanctuary that enjoys a unique status in our constitutional jurisprudence," that the registry was an opt-in program that "puts the choice of whether . . . to restrict commercial calls entirely in the hands of the consumers," and that the registry "materially" furthered the government's interests—that led it to conclude that there was a "reasonable fit" between the regulation and the government's interest.[207] The proposed "do not nag" mechanism arguably shares the same four characteristics: "Do not nag" would not prohibit companies from communicating with their customers through notifications and reminders; it would only specify guidelines for what this communication would look like.

It is important to note, though, that there is a key difference between the relationships between consumers and telemarketers in the case of the "do not call" registry and the relationships between consumers and nagging companies: In the nagging context, the companies engaging in the nagging may have an existing commercial or even contractual relationship with the consumer, which is not the case when it comes to telemarketing calls.[208] That said, like the "do not call" registry, "do not nag" places the choice of whether to restrict nagging with the consumer, not the government.

2. *Overburdening Consumers.* — Another possible critique of a "do not nag" feature is that it puts the onus on the consumer. Because online companies, particularly those with significant market power, can so easily circumvent the need to obtain consumers' consent,[209] some might view an opt-in solution that places the choice of whether to receive repeated communications or interactions in the hands of consumers as impractical or overly optimistic about consumers' ability to understand and express their preferences.

Such concerns, though understandable, are unfounded. First, there is already an example of an opt-in solution—the "do not call" registry—that works. Consumers have experience putting themselves on a registry, even with the "very strong 'status quo' bias";[210] after all, millions of people have opted into the "do not call" list.[211] The more challenging task in rolling out "do not nag" will likely be making sure that consumers know about it, but, again, this task is one that regulators have successfully taken on before: "From its inception, the Do Not Call Registry was heavily publicized, and the public responded."[212] Moreover, a solution that doesn't place the onus on the consumer will raise difficult line-drawing problems that may, in many cases, be unsolvable simply because it will often be

207. *Mainstream Mktg. Servs.*, 358 F.3d at 1233.

208. Luguri & Strahilevitz, supra note 6, at 101.

209. See supra section I.B.1.

210. Sunstein & Thaler, Libertarian Paternalism, supra note 42, at 176.

211. See supra note 178.

212. Willis, supra note 12, at 108.

impossible to distinguish between a repetitive communication that is harmful and one that is acceptable or even desirable.[213]

3. Unintended Effects. — Policymakers should be cognizant of any potential negative second- and third-order effects of a "do not nag" mechanism on consumers. As Professor Gus Hurwitz notes, "[T]he reality of design is that it is hard to do well and the effects of simple design decisions can be complex and difficult to predict . . . . [M]andating alternative designs may, in fact, yield substantially worse effects for many users."[214] Professor David Pozen's conception of "privacy–privacy tradeoffs," which occur when an intervention designed to protect one form of privacy can actually "jeopardize another form of privacy," is potentially useful here.[215] Regulated companies "may respond to a new measure by shifting to different practices" that could be as or more harmful to consumers than nagging.[216]

An effective solution to the problem of nagging therefore should not prompt companies to engage in new or different pernicious design practices—or, at least, practices that would be immune to regulation or intervention. For example, if a significant number of consumers opt into the "do not nag" scheme and companies find that they can no longer rely on nags as a design tactic to influence consumers, will companies turn to other categories of dark patterns, such as sneaking or interface interference,[217] instead? Could an attempt to solve the problem of persistent digital intrusions unwittingly unleash a proliferation of manipulative or deceptive design? Even if the answer to these questions is yes, however, the FTC arguably already has tools at its disposal to fight the other categories of dark patterns, which tend to involve some amount of deception, that would likely replace nagging through its existing section 5 authority.[218] Finally, the benefit of implementing an opt-in solution like "do not nag" is that regulators may not have to resolve these potential tradeoffs for consumers at all. Rather, just as the opt-in TSA Pre-Check program gives travelers the option to resolve their own "privacy–privacy tradeoffs,"[219] a "do not nag" feature places the power to weigh tradeoffs between different digital interactions into the hands of consumers.

CONCLUSION

Although aggressive marketing tactics and strategically designed interactions are not new, in the digital age, firms can deploy them at an unprecedented scale to influence consumers' behavior and choices.

213. See supra section II.B.3.

214. Hurwitz, supra note 7, at 104.

215. David E. Pozen, Privacy–Privacy Tradeoffs, 83 U. Chi. L. Rev. 221, 232 (2016).

216. Id.

217. See supra note 19 and accompanying text.

218. See supra notes 99–102 and accompanying text.

219. Pozen, supra note 215, at 244.

Thanks to rapid, continual technological innovation, companies have the ability to reach consumers in ever-more targeted and persuasive ways; regulators and courts are no strangers to wrestling with the question of whether and how to rein in these new business practices. Design plays a critical role in framing firms' interactions with consumers, and dark patterns—online design practices that influence consumers to do things they otherwise wouldn't—are attracting increasing attention from legislators, regulators, and scholars.

But one category of dark patterns—nagging, which relies on persistent, repeated interactions to influence the consumer—has largely evaded close scrutiny thus far. Consumers encounter nags everywhere, and nags hurt consumer welfare by undermining consumers' consent, causing attentional intrusions, and, more indirectly, facilitating privacy harms and anticompetitive conduct. Existing consumer protection law, however, is unlikely to reach a design practice like nagging, given the relatively narrow definition of cognizable injuries. The problem of nagging thus requires a more tailored solution—one that can curb the practice without being overly rigid or prescriptive, especially considering the First Amendment protection of commercial speech as well as the difficulty of ascertaining consumers' preferences and the choices that align with those preferences. A "do not nag" feature, modeled off the national "do not call" registry, is a promising intervention because it puts the choice of whether to stop receiving nags in consumers' hands and is likely to withstand First Amendment challenges. While existing consumer protection law may be inadequate to meaningfully address some of the new harmful strategies through which companies can interact with consumers in the digital economy, policymakers may be able to adapt and repurpose creative interventions that have successfully curbed similar pre–digital era practices to tackle these new problems.