

Intellectual Property & Technology Law Journal

Edited by the Technology and Proprietary Rights Group of Weil, Gotshal & Manges LLP

VOLUME 35 • NUMBER 4 • APRIL 2023

Potential First Amendment Defenses to a Dark Patterns Claim

By Stephen J. Newman, Allen H. Denson and Jimmy L. Ma

Courts and the Federal Trade Commission (the FTC) have not yet addressed whether and to what degree the First Amendment of the U.S. Constitution may protect advertising techniques that make use of supposed “dark patterns.”¹ Although the FTC held a workshop² on dark patterns in April 2021 and subsequently issued a more detailed report, there is no specific regulation governing which practices are unlawful or under what circumstances. However, any attempt to regulate internet speech – including the FTC’s attempt to police dark patterns through use of the FTC Act – must satisfy the four-part test set forth by the U.S. Supreme Court in *Sorrell v. IMS Health Inc.*,³ which sets forth a framework for constitutional protection of commercial speech.

COMMERCIAL SPEECH

Under *Sorrell*, a content-based regulation on non-misleading commercial speech that relates to lawful activity does not violate the First Amendment if: (1) the government has substantial interest to be achieved by regulation; (2) the regulation directly advances that governmental interest; and (3) the regulation is narrowly tailored so as to not restrict more speech than is necessary.⁴ Academics⁵ have acknowledged that an otherwise dark pattern’s use of truthful information merits protection under the First Amendment.⁶ The U.S. Supreme Court acknowledges a broad definition of speech to include words, images and data, noting that “the creation and dissemination of information are speech within the meaning of the First Amendment,” and “an individual’s right to speak is implicated when information he or she possesses is subjected to restraints on the way in which the information might be used or disseminated.”⁷

DARK PATTERNS

The FTC brought two actions against Vonage and Epic Games regarding dark patterns, both of which settled for nine figures. These cases arguably involved misleading practices that probably would be acknowledged as misleading under longstanding deception law, and therefore they do not raise any major First Amendment concerns. According

Stephen J. Newman (snewman@stroock.com) is a partner at Stroock & Stroock & Lavan LLP handling class action defense and other representative litigation, including multidistrict cases, as well as proceedings launched by government officials on behalf of the general public. Allen H. Denson (adenson@stroock.com) is a partner at the firm representing financial institutions that are defending against financial regulators that challenge their marketing, lending and collection practices. Jimmy L. Ma (jlma@stroock.com) is an associate at the firm.

to the FTC's complaint, Vonage allegedly used dark patterns to make it difficult for customers to cancel their services and charged unexpected early termination fees. Meanwhile, Epic Games allegedly employed dark patterns in the popular game Fortnite to charge consumers for certain in-game items, usually purchased by kids, without obtaining express informed consent from the account owners, and then precluded them from accessing previously purchased content when they disputed unauthorized charges.

University of Chicago Law School Professor Lior Strahilevitz, a panelist at the FTC's dark patterns workshop, has argued that the First Amendment would not protect the following conduct:

- False or misleading positive reviews from consumers, notices that other individuals are purchasing the product, or that a sale will end soon;
- Adding items in a consumer's cart without authorization;
- Selling different items to the customer than what was advertised;
- Tricking consumers into sharing personal information or registering; and
- Unanticipated and/or unauthorized automatic renewals.⁸

In one study, academics used automated technology to assess 11,000 shopping websites and identify, measure, and study dark patterns, focusing specifically on websites that used the following deceptive practices:

- Sneaking products into users' shopping carts without their consent;
- Adding hidden costs as users are about to complete a purchase;
- Adding hidden subscription charges under the pretense of a one-time fee or free trial;
- Using false countdown timers for deals when in fact such offers remained valid after the expiration time;

- Using customer testimonials regarding products or services where the testimonial's source could not be validated based on a search on Google or because the dark pattern website lacked a form to submit testimonials; and
- Utilizing "low-stock" messages that deceptively signaled to users about limited quantities of a product but in fact decreased stock amounts in a recurring, deterministic pattern according to a schedule or that randomly generated stock values.⁹

Compliance professionals should be aware that government agencies may utilize such automated technology to identify and target dark patterns, especially deceptive practices that go beyond the protections of the First Amendment. Given the increasing ease of scanning large numbers of websites through automation seeking particular examples of dark patterns marketing, even websites with low engagement may find themselves subject to scrutiny, either from a government enforcer or a private litigant.

"Nagging" and "Confirmshaming"

Aggressive prosecution of dark patterns claims may have limits, however. The First Amendment may invalidate attempts to challenge dark patterns that are deemed unfair but that involve no false or deceptive statements. One such example is "nagging," a practice of repeatedly requesting a consumer to do something that may include asking a consumer to agree to certain terms and conditions, to turn on notifications, or to reconsider their previous choices.

Another example is confirmshaming, which is the use of language and guilt to steer users away from making a certain choice (e.g., "No thanks, I hate saving money" and "No thanks, I hate fun and games."). Although the FTC has broad statutory power to combat "unfair or deceptive" practices,¹⁰ the First Amendment may limit the FTC's ability to prohibit advertising conduct on the grounds that it is excessively persuasive. Nagging and confirmshaming may be lawful because they are nondeceptive, and it is not clear how persuasive advertising techniques are unfair because they cause or are likely to cause "substantial injury" to consumers.¹¹

At most, nagging and confirmshaming may be said to be annoying to a consumer, but such “injury” is hardly substantial; annoyance is not coercion. If it were, many advertising jingles that became unshakeable earworms could have been prohibited long ago. As such, both nagging and confirmshaming may be protected by the First Amendment.

At most, nagging and confirmshaming may be said to be annoying to a consumer, but such “injury” is hardly substantial; annoyance is not coercion.

Furthermore, there are doubts as to whether the government has a substantial interest over regulation of dark patterns on the grounds that they are unduly persuasive. In a related context, courts have upheld the FTC’s national “do not call” registry – a registry that restricted sales calls – based on the substantial government interest in protecting against speech that invades the privacy of the home, but such interest likely does not apply here.¹² Unlike the consumer’s relationship with a telemarketer, the consumer usually accesses a website and thereby initiates a relationship with the nagging or confirmshaming company. In sum, courts may scrutinize dark patterns enforcement theories to the extent they are pursued aggressively against practices that do not involve false or misleading statements of fact.¹³

FIRST AMENDMENT CHALLENGES

Some trade organizations have raised First Amendment concerns regarding similar issues. For example, in October 2020, the California attorney general proposed privacy regulations intended to make it easier for consumers to opt out of information sharing.¹⁴ These proposed regulations were ultimately implemented, finalized, and renumbered under California Code Regulations, Title 11, § 7026. During the public comment period, however, the Consumer Data Industry Association (CDIA) criticized the proposed rule for Section 7026(h)(2) because it banned businesses from using “confusing language” when the consumer tries to opt out without clarifying the meaning of “confusing,” and therefore such law unconstitutionally “prohibit[s] an undefined category of speech.”¹⁵ Similarly, the CDIA pointed out that the proposed rule for

Section 7026(h)(3)’s restriction on businesses from requiring consumers to click through “or listen to reasons not to opt out” (i.e., confirmshaming) is also a content restriction that, without any further guidance, raises First Amendment concerns.¹⁶

A group of seven leading advertising and marketing trade associations have also argued that as a result of the proposed rule for Section 7026(h)(3)’s restrictions, “consumers’ receipt of factual, critical information about the nature of the ad-supported Internet would be unduly hindered, thereby undermining a consumer’s ability to make an informed decision” and raising First Amendment concerns.¹⁷ It has yet to be seen whether the above First Amendment challenges will be raised against these or other similar laws.

Effective on January 1, 2024, California’s Age-Appropriate Design Code Act (AADC) will impose rules governing advertising to children under the age of 18.¹⁸ Courts can be expected to find that the AADC withstands First Amendment concerns based on the law’s targeting of specifically-defined deceptive practices and because there is a more substantial government interest in protecting children, as children may be particularly susceptible to manipulative advertising techniques and less able to protect themselves from harm online.

To the extent First Amendment protections do not apply, website operators may also be liable for content involving any unlawful dark patterns created by third parties. Although Section 230 of the Communications Decency Act immunizes website operators from liability for content published by third parties on those websites, the U.S. Court of Appeals for the Ninth Circuit held that Section 230 does not apply where the website operator utilizes designs that materially contribute to a content’s unlawfulness, such as designing pre-populated drop-down answers, search mechanisms, or email notification systems that are based on discriminatory criteria.¹⁹

The regulatory landscape and jurisprudence regarding the applicability of the First Amendment to dark patterns are still evolving.

Notes

1. See Fed. Trade Comm’n, *Bringing Dark Patterns to Light* (Sept. 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.

2. FTC Dark Patterns Workshop (Apr. 29, 2021), available at https://www.ftc.gov/system/files/documents/public_events/1586943/ftc_darkpatterns_workshop_transcript.pdf.
3. 564 U.S. 552, 579 (2011).
4. Sorrell, 564 U.S. at 572, 579 (citing *Central Hudson Gas & Electric Corporation v. Public Service Commission of New York (Central Hudson)*, 447 U.S. 557, 566 (1980)).
5. See Jamie Luguri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 *J. Legal Analysis* 43, 99–100 (2021).
6. As originally published, we attributed this view also to “even the man who coined the term ‘dark patterns,’” Harry Brignull, based on his statement to the FTC at its April 2021 Dark Patterns Workshop that if statements embedded in what otherwise might be called dark patterns “are actually true, then that’s honest marketing. In fact, it’s really useful for [inaudible in transcript, probably people] to know that information.” We understood that statement to reflect support for the First Amendment principle that truthful information should not be suppressed for the sake of achieving some other public policy goal. After publication, we exchanged emails with Dr. Brignull, who asked us to clarify that he is not an attorney or a legal scholar, and thus he is not in a position to have a meaningful opinion on questions of law. We thank Dr. Brignull for his input.
7. Sorrell, 564 U.S. at 568–70 (striking down a law that restricted the disclosure, sale and use of pharmacy records that revealed the prescribing practices of individual doctors).
8. See Jamie Luguri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 *J. Legal Analysis* 43, 53, 99–101 (2021).
9. Arunesh Mathur et al., *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 81 (November 2019), available at <https://doi.org/10.1145/3359183>.
10. 15 U.S.C. § 45(a) (2018).
11. See FTC Policy Statement on Unfairness, FTC (Dec. 17, 1980), <https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness> (“In most cases a substantial injury involves monetary harm, as when sellers coerce consumers into purchasing unwanted goods or services. . .”).
12. Alison Hung, *Keeping Consumers in the Dark: Addressing ‘Nagging’ Concerns and Injury* (January 19, 2021). *Columbia Law Review*, Vol. 121, No. 8, at 2507 (2021).
13. The Supreme Court emphasizes that “[t]he First Amendment directs [courts] to be especially skeptical of regulations that seek to keep people in the dark for what the government perceives to be their own good.” 44 *Liquormart, Inc. v. Rhode Island*, 517 U.S. 484, 503 (1996) (striking down a state law prohibiting the advertising of alcohol prices because the right of consumers to receive truthful product information about prices was protected speech and because the state interest in promoting temperance was not narrowly drawn enough to prevent consumers from receiving lawful and truthful information about prices); see also Sorrell, 564 U.S. at 568–70.
14. <https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-notice-of-third-mod-101220.pdf>.
15. <https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-written-comm-3rd-15-day-period.pdf>.
16. <https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-written-comm-3rd-15-day-period.pdf>.
17. *Id.*; see also 44 *Liquormart, Inc.*, 517 U.S. at 503.
18. Cal. Civ. Code § 1798.99.31(b)(7) (prohibiting a business that provides an online service, product, or feature likely to be accessed by children from using “dark patterns” to get children to provide personal information, forego privacy protections, or to take any action that is “materially detrimental to the child’s physical health, mental health, or well-being”); see also *id.* § 1798.140(k) (defining dark patterns as “a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice, as further defined by regulation”).
19. See, e.g., *Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1169–70 (9th Cir. 2008) (holding that Section 230 did not apply to roommate-matching website that was designed to force subscribers to divulge protected characteristics and discriminatory preferences and to match those who had rooms with those who were looking for rooms based on criteria that appeared to be prohibited by Fair Housing Act).

Copyright © 2023 CCH Incorporated. All Rights Reserved.
Reprinted from *Intellectual Property & Technology Law Journal*, April 2023, Volume 35,
Number 4, pages 9–12, with permission from Wolters Kluwer, New York, NY,
1-800-638-8437, www.WoltersKluwerLR.com

