AMERICAN CIVIL LIBERTIES UNION FOUNDATION

Speech, Privacy, and Technology Project
ACLU National Legal Department

April 13, 2026

SUBMITTED VIA REGULATIONS.GOV

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Ave. NW
Ste. CC-5610 (Annex B)
Washington, DC 20580

Re: Advanced Notice of Proposed Rulemaking—Negative Option Rule, RIN 3084-AB54

Dear Chairman Ferguson,

We write to you on behalf of the American Civil Liberties Union Foundation ("ACLU") in response to the Advance Notice of Proposed Rulemaking and Request for Public Comment ("ANPRM") released by the Federal Trade Commission ("FTC" or "the Commission") on March 13, 2026. In the ANPRM, the Commission seeks comments on ways to improve its existing regulations for negative option plans including potentially adopting all or part(s) of the rule entitled "Negative Option Rule,"[1] promulgated on November 15, 2024 and subsequently vacated by the United States Court of Appeals for the Eighth Circuit ("the Vacated Rule").

The ACLU is a nationwide, nonpartisan, nonprofit organization dedicated to the principles of liberty, privacy, equality, and rights of individuals embodied in the Constitution and our nation's civil rights laws. With more than four million members, activists, and supporters, the ACLU has worked in all 50 states, Puerto Rico, and Washington, D.C., to strengthen the fundamental American value of privacy, and in doing so has developed expertise in consumer data collection, sale, and exposure;[2] consumer choice and "dark patterns";[3] and privacy issues related to emerging technologies.[4]

---

[1] Negative Option Rule, 89 Fed. Reg. 90476 (Nov. 15, 2024).
[2] Letter from Christopher Anders, Fed. Pol'y Dir., ACLU, to House Energy & Com. Comm. on Am. Data Priv. Prot. Act (July 18, 2022), https://www.aclu.org/documents/aclu-letter-house-energy-and-commerce-committee-american-data-privacy-protection-act.
[3] ACLU Statement on Am. Data Priv. Prot. Act, Ahead of Comm. Markup (July 18, 2022), https://www.aclu.org/documents/aclu-statement-american-data-privacy-protection-act-ahead-committee-markup.
[4] *ACLU v. Clearview AI*, ACLU (last updated May 11, 2022), https://www.aclu.org/cases/aclu-v-clearview-ai; *Carpenter v. United States*, ACLU (last updated June 22, 2018), https://www.aclu.org/cases/carpenter-v-united-states; Jay Stanley, *Utah Passes Nation's Strongest Digital Identity Bill*, ACLU (Mar. 30, 2026), https://www.aclu.org/news/privacy-technology/utah-digital-id-law; Ivey Dyson & Jacob Snow, *The Federal Trade Commission Must Investigate Meta and X for Complicity with Government Surveillance*, ACLU (Dec. 12, 2023), https://www.aclu.org/news/privacy-technology/the-federal-trade-commission-must-investigate-meta-and-x-for-complicity-with-government-surveillance.

Our comments draw from these experiences to demonstrate how negative option practices obstruct consumer choice, thereby causing meaningful privacy-related harm to Americans in a range of ways. To target these issues, we address why the FTC should:

- Broadly re-institute the Vacated Rule with certain adjustments, summarized below;
- Create clear, concrete standards and requirements around verification, authentication, or confirmation at cancellation;
- Explicitly ban and define "dark patterns" in consent and cancellation, increasing the enforceability of a potential rule against unfair and deceptive practices.

We encourage the FTC to address these damaging practices in this rulemaking and thank Chairman Ferguson for his leadership on this topic.

1. The Consumer Harms Caused by Negative Option Practices Merit Action from the FTC

Negative Option Practices Hurt Consumer Choice and Harm Privacy

The Commission's renewed attention to negative option practices arrives at a pivotal moment. The deployment of negative option practices outside of an adequate consent, disclosure, accuracy, and cancellation regime damages consumer choice, thereby exacerbating existing privacy harms.

Negative options are practices where service providers, after having signed someone up for a free trial or paid service, start or continue to charge the customer and hold them to contract terms; this is predicated on the assumption that, because the customer has not explicitly cancelled their agreement, they continue to consent. This approach can cause meaningful harm to consumers when companies make insufficient disclosures, charge customers without legitimate consent, and impede attempts to cancel.

The Commission has highlighted ways in which these unfair and deceptive practices create consumer choice and competition concerns, but they also exacerbate existing privacy issues. Many commercial and non-commercial entities collect or derive massive amounts of information about the people who interact with them, including data about religion, health history, relationships, career, and—for both adults and minors—gender, age, and location. Collecting entities can easily monetize this data by selling it or running ads; this creates an incentive to leverage these tactics. Negative option practices cause yet further damage through data breaches and the distribution or capture of data, from targeted and real-time advertising, to acquisition by data brokers and bad actors—exposing consumers to exacerbated risks of harm.

Consumer preferences can only be meaningfully ascertained by express or opt-in consent without

pressure or manipulation. Unfair or deceptive negative option practices allow companies to continue monetizing consumers' information without their authentic consent and place enormous burdens on those who wish to protect their data. The "dark patterns" that enable these practices disproportionately impact those who often do not have sufficient time or knowledge to oppose them, including the elderly[5] and children.[6]

Such practices are also, unfortunately, rewarded by market conditions in which an individual's data can be worth as much or more than the subscription they pay for.[7] This incentive means unfair negative option tactics serve additionally as unfair data practices for many companies.

The FTC's own docket from 2025 contains examples of how these practices drive privacy harms. For example, Uber is a rideshare and food delivery app against which the FTC has taken action because the company allegedly "charged consumers for its Uber One subscription service without their consent . . . and made it difficult for users to cancel the service."[8] Uber has stated that it discloses "user personalized information" for ads in a way that can be legally categorized as a "sale."[9] The company leverages real-time location, commute, and current destination information,[10] specific purchase information,[11] financial details,[12] certain demographic details,[13] and a range of other characteristics to deliver targeted and real-time advertisements—and markets these data categories to prospective advertisers. This practice has proven lucrative; Uber predicts

[5] Pavithren S/O V S Pakianathan, Towards Inclusive Design of Mobile Privacy and Security for Older Adults (Aug. 2021), https://www.researchgate.net/profile/Pavithren-V-S-Pakianathan/publication/354462634_Towards_Inclusive_Design_of_Mobile_Privacy_and_Security/links/6139bb3deb7d6b0b5329454f/Towards-Inclusive-Design-of-Mobile-Privacy-and-Security.pdf.
[6] René Schäfer et al., *Growing Up With Dark Patterns: How Children Perceive Malicious User Interface Designs*, Proc. of the 13th Nordic Conf. on Human-Computer Interaction, Oct. 2024, https://dl.acm.org/doi/abs/10.1145/3679318.3685358.
[7] James E. Short & Steve Todd, *What's Your Data Worth?*, 58 MIT Sloan Mgmt. Rev. 17 (2017), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/short-whats-your-data-worth.pdf; Ben Wolford, *What's Your Data Really Worth? (2025 Update)*, Proton Blog (Feb. 8, 2024), https://proton.me/blog/what-is-your-data-worth; Press Release, Meta, Meta Reports Fourth Quarter and Full Year 2025 Results (Jan. 28, 2026), https://investor.atmeta.com/investor-news/press-release-details/2026/Meta-Reports-Fourth-Quarter-and-Full-Year-2025-Results/default.aspx.
[8] *FTC v. Uber*, FTC (last updated Dec. 15, 2025), https://www.ftc.gov/legal-library/browse/cases-proceedings/2423092-uber-ftc-v.
[9] Uber, *U.S. User Data Rights*, https://perma.cc/E37G-44NP.
[10] Uber, *Advertising*, https://www.uber.com/us/en/advertising/audience/.
[11] *Id.*
[12] *Id.*
[13] Uber, *Ads Overview and Settings*, https://help.uber.com/en/riders/article/ads-overview-and-settings?nodeId=f7cf6e0a-41c4-4a1c-8e06-15864bd19850.

over $2 billion in annualized advertising revenue for 2026.[14] Ensuring that consumers are captive helps ensure that companies can extract and monetize this highly valuable data.

Similarly, Amazon, which the Commission recently settled with for deceptive signups and subscriptions that "feel impossible to cancel,"[15] reports capturing and retaining dozens[16] of categories of consumer data. This massive dataset includes "information that may reveal . . . sexual orientation, or other protected classifications," whether someone chooses to "create a child profile, baby registry, or wedding registry," "network activity," "audio or visual information," and "geolocation data."[17] The e-commerce giant uses its data repository to deliver "behavioral ads"[18] and individualize pricing to maximize sales.[19]

And, even if a consumer does not directly use the service while their contract is artificially extended, their continued presence on customer lists and the perpetuation of contract terms allows monetization to continue. Entities can use these tactics to create unfair competitive advantages with advertising customers by inflating market share. Furthermore, they can expand the period during which they can contractually retain personal data; several jurisdictions require deletion of data or mandate the conclusion of retention once data is no longer active or necessary. This means companies can leverage negative option tactics to evade regulatory requirements and monetize individuals' data for longer than the individuals would otherwise consent to or allow.

Consumers coerced, manipulated, or deceived into agreement and continuing "consent" cannot therefore reasonably avoid the damage done to their privacy.

---

[14] Uber, 2026 Proxy Statement and Notice of Annual Meeting of Stockholders 10, 58 (2026), https://s23.q4cdn.com/407969754/files/doc_events/2026/May/04/Uber-2026-Proxy-Web-Ready-Version.pdf.
[15] Press Release, FTC, FTC Secures Historic $2.5 Billion Settlement Against Amazon (Sept. 25, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/09/ftc-secures-historic-25-billion-settlement-against-amazon.
[16] Amazon, *Additional State-Specific Privacy Disclosures* (Sept. 30, 2025), https://www.amazon.com/gp/help/customer/display.html?nodeId=GC5HB5DVMU5Y8CJ2.
[17] *Id.*
[18] Amazon, Buy With Prime, *Your Ads Privacy Choices*, https://buywithprime.amazon.com/your-ads-privacy-choices.
[19] Amazon, *Simplify Your Pricing Strategy*, https://sell.amazon.com/tools/automate-pricing; Julia Angwin & Surya Mattu, *Amazon Says It Puts Customers First. But Its Pricing Algorithm Doesn't*, ProPublica (Sept. 20, 2016), https://www.propublica.org/article/amazon-says-it-puts-customers-first-but-its-pricing-algorithm-doesnt; Anu Kaggadasapura et al., *How Generative AI and Data are Redefining Retail Experiences*, Amazon Web Servs. (Oct. 22, 2024), https://aws.amazon.com/blogs/industries/how-generative-ai-and-data-are-redefining-retail-experiences/.

Privacy damage caused by unfair or deceptive negative option tactics exacerbates data security and safety risks.

The boost to data harvesting driven by negative option tactics exacerbates the serious harms already generated by the personal data collection ecosystem—including exposing Americans' data to bad actors. We here highlight three major pathways by which these data harms accrue.

Data breaches are the first pathway through which this damage occurs. Neither few nor far between,[20] these hacks, exploits, and vulnerabilities "cause financial loss"[21] and empower a broad array of criminal activity including identity theft, fraud, extortion, and doxxing.[22] Many of the same entities identified by the FTC and other regulators as using deceptive billing or cancellation practices have had major breaches or data security failures with consumer or business data, including Uber,[23] Amazon,[24] Adobe,[25] Chegg,[26] and Match Group.[27] And, Cleo AI—which the FTC and Chairman Ferguson also identified as using negative option practices[28]—is built on

[20] Priv. Rts. Clearinghouse, *Data Breaches*, https://privacyrights.org/data-breaches.
[21] Cybersecurity & Infrastructure Sec. Agency, *Protecting Sensitive and Personal Information from Ransomware-Caused Data Breaches*, https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Protecting_Sensitive_and_Personal_Information_from_Ransomware-Caused_Data_Breaches-508C.pdf.
[22] Europol, *Steal, Deal, Repeat: Cybercriminals Cash in on Your Data*, https://www.europol.europa.eu/media-press/newsroom/news/steal-deal-repeat-cybercriminals-cash-in-your-data; Fed. Bureau of Investigation, *The Cyber Threat*, https://www.fbi.gov/investigate/cyber.
[23] Dave Lewis, *Uber Suffers Data Breach Affecting 50,000*, Forbes (Feb. 28, 2015), https://www.forbes.com/sites/davelewis/2015/02/28/uber-suffers-data-breach-affecting-50000/; Dara Khosrowshahi, *2016 Data Security Incident*, Uber Newsroom (Nov. 21, 2017), https://www.uber.com/us/en/newsroom/2016-data-incident/; Kate Conger & Kevin Roose, *Uber Investigating Breach of Its Computer Systems*, N.Y. Times (Sept. 15, 2022), https://www.nytimes.com/2022/09/15/technology/uber-hacking-breach.html; *see also FTC v. Uber*, supra note 8.
[24] Theo Leggett, *Amazon Hit With $886m Fine for Alleged Data Law Breach*, BBC (July 30, 2021), https://www.bbc.com/news/business-58024116; *see also* Press Release, FTC, *supra* note 15.
[25] Chris Welch, *Over 150 Million Breached Records from Adobe Hack Have Surfaced Online*, The Verge (Nov. 7, 2013), https://www.theverge.com/2013/11/7/5078560/over-150-million-breached-records-from-adobe-hack-surface-online; Paul Bischoff, *7 Million Adobe Creative Cloud Accounts Exposed to the Public*, Comparitech (Jan. 3, 2020), https://www.comparitech.com/blog/information-security/7-million-adobe-creative-cloud-accounts-exposed-to-the-public/; Press Release, FTC, FTC Takes Action Against Adobe and Executives for Hiding Fees, Preventing Consumers from Easily Cancelling Software Subscriptions (June 17, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/06/ftc-takes-action-against-adobe-executives-hiding-fees-preventing-consumers-easily-cancelling.
[26] *Chegg Data Breach*, Have I Been Pwned, https://haveibeenpwned.com/Breach/Chegg; *Chegg, Inc.*, FTC (last updated Sept. 15, 2025), https://www.ftc.gov/legal-library/browse/cases-proceedings/c4782-chegg-inc.
[27] Pieter Arntz, *Match, Hinge, OkCupid and Panera Bread Breached by Ransomware Group*, MalwareBytes Labs (Jan, 30, 2026), https://www.malwarebytes.com/blog/news/2026/01/match-hinge-okcupid-and-panera-bread-breached-by-ransomware-group.; Press Release, FTC, FTC Takes Action Against Match and OkCupid for Deceiving Users by Sharing Personal Data With Third Party (Mar. 30, 2026), https://www.ftc.gov/news-events/news/press-releases/2026/03/ftc-takes-action-against-match-okcupid-deceiving-users-sharing-personal-data-third-party.
[28] U.S. H.R., *Testimony of the Federal Trade Commission Before the Committee on Appropriations Subcommittee on Financial Services and General Government* (May 15, 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-Chairman-Andrew-N-Ferguson-FSGG-Testimony-05-15-2025.pdf; *FTC v. Cleo AI, Inc.*, No. 25-cv-2594 (S.D.N.Y.).

OpenAI's GPT models; researchers and security organizations have repeatedly[29] shown that these models are vulnerable to many different attacks that can extract information, with new methods being discovered as recently as March 2026.[30]

Second, privacy harms may occur through data misuse. As the FTC discovered, Match Group shared its collected data with an entity that used the data to develop facial recognition technology for foreign governments—during the same period when it was deploying unfair cancellation prevention tactics.[31]

The third, more formal, mechanism of data exposure also exacerbates risk and harm: advertising. As the Commission is aware through its work on real-time bidding (RTB)[32] and targeted advertising,[33] the largest data collection organizations distribute data through advertising—including companies identified by the FTC for preventing cancellation like Amazon,[34] Chegg,[35] LA Fitness,[36] and Uber.[37] This data is often shared with, or captured by, data brokers—companies that collect, infer, cross-reference, combine, and sell personal data.[38] And, while the data used or

---

[29] Moshe Bernstein & Liv Matan, *HackedGPT: Novel AI Vulnerabilities Open the Door for Private Data Leakage*, Tenable (Nov. 5, 2025), https://www.tenable.com/blog/hackedgpt-novel-ai-vulnerabilities-open-the-door-for-private-data-leakage.

[30] Check Point Rsch., *ChatGPT Data Leakage Via a Hidden Outbound Channel in the Code Execution Runtime*, https://research.checkpoint.com/2026/chatgpt-data-leakage-via-a-hidden-outbound-channel-in-the-code-execution-runtime/.

[31] Jon Brodkin, *OkCupid Gave 3 Million Dating-App Photos to Facial Recognition Firm, FTC Says*, ArsTechnica (Mar. 31, 2026), https://arstechnica.com/tech-policy/2026/03/okcupid-match-pay-no-fine-for-sharing-user-photos-with-facial-recognition-firm/; Press Release, FTC, Match Group Agrees to Pay $14 Million, Permanently Stop Deceptive Advertising, Cancellation, and Billing Practices to Resolve FTC Charges (Aug. 12, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/08/match-group-agrees-pay-14-million-permanently-stop-deceptive-advertising-cancellation-billing.

[32] Press Release, FTC, FTC Finalizes Order Banning Mobilewalla from Selling Sensitive Location Data (Jan. 14, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-order-banning-mobilewalla-selling-sensitive-location-data.

[33] Yan Lau, A Brief Primer on the Economics of Targeted Advertising (Jan. 2020), https://www.ftc.gov/reports/brief-primer-economics-targeted-advertising.

[34] Amazon Ads, *What is Real-Time Bidding (RTB)? Definition and Importance*, https://advertising.amazon.com/library/guides/real-time-bidding; *see also* Press Release, FTC, *supra* note 15.

[35] Kimberly Maul, *Chegg Uses Data to Connect College Students With Brands*, Ad Exchanger (June 3, 2013), https://www.adexchanger.com/data-exchanges/chegg-uses-data-to-connect-college-students-with-brands/; Chegg, *Chegg Privacy Policy* (Jan. 9, 2026), https://www.chegg.com/en-US/privacypolicy; *see also FTC v. Chegg, Inc.*, No. 25-cv-7827 (N.D. Cal.).

[36] LA Fitness, *Your Privacy Options*, https://shoplafitness.com/pages/data-sharing-opt-out; Press Release, FTC, FTC Sues LA Fitness for Making it Difficult for Consumers to Cancel Gym Memberships, https://www.ftc.gov/news-events/news/press-releases/2025/08/ftc-sues-la-fitness-making-it-difficult-consumers-cancel-gym-memberships.

[37] Jacob Tsafatinos et al., *Real-Time Exactly-Once Ad Event Processing with Apache Flink, Kafka, and Pinot*, Uber Blog (Sept. 22, 2021), https://www.uber.com/us/en/blog/real-time-exactly-once-ad-event-processing/; *see also FTC v. Uber*, supra note 8.

[38] Lena Cohen, *Online Behavioral Ads Fuel the Surveillance Industry—Here's How*, Elec. Frontier Found. (Jan. 6, 2025), https://www.eff.org/deeplinks/2025/01/online-behavioral-ads-fuel-surveillance-industry-heres-how; Dr

shared with third parties for advertising is sometimes referred to as "anonymous," research[39] and real-world instances (some detailed below) have shown repeatedly that anonymized data is easily re-identifiable at sometimes extremely high rates.[40]

Even if targeted advertising is done in a way that does not violate civil rights or other laws, the extractive elements of ad targeting, and the extent of data collection and exposure they incentivize, create troubling outcomes.

Researchers estimate that over 100 trillion instances of real-time bidding data exposure occur every year,[41] estimates indicate that the majority of people in America have been the victims of multiple breaches,[42] and victims of identity theft are more than twice as likely (versus nonvictims) to have experienced a data breach.[43] Personal data collected from real-time bidding and passed through brokers was re-identified and used to harass a member of the clergy[44] and to track American security and defense personnel.[45] A number[46] of organizations and researchers have raised the alarm over data broker information being used in the stalking of domestic violence survivors.[47]

In summation, unfair and deceptive negative option practices increase risk and harm to privacy, data security, and consumer choice.

Johnny Ryan FRHistS & Wolfie Christl, America's Hidden Security Crisis, Irish Council for C.L., https://www.iccl.ie/wp-content/uploads/2023/11/Americas-hidden-security-crisis.pdf.

[39] Natasha Lomas, *Researchers Spotlight the Lie of 'Anonymous' Data*, TechCrunch (July 24, 2019), https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data; Isla Sibanda, *Reidentifying the Anonymized: Ethical Hacking Challenges in AI Data Training*, ISACA (Sept. 16, 2024), https://www.isaca.org/resources/news-and-trends/industry-news/2024/reidentifying-the-anonymized-ethical-hacking-challenges-in-ai-data-training; TorGuard, *Unmasking the Web: How Ad Tracking, Analytics, and AI are De-Anonymizing Users* (Oct. 8, 2025), https://blog.torguard.net/ad-tracking-analytics-ai-de-anonymizing-users/; Nicolás Torres & Patricio Olivares, *De-Anonymizing Users Across Rating Datasets via Record Linkage and Quasi-Identifier Attacks*, Data, 2024, https://www.mdpi.com/2306-5729/9/6/75.

[40] Luc Rocher et al., *Estimating the Success of Re-identifications in Incomplete Datasets Using Generative Models*, Nature Commc'ns, July 2017, https://www.nature.com/articles/s41467-019-10933-3.

[41] EPIC, *Online Advertising & Tracking*, https://epic.org/issues/consumer-privacy/online-advertising-and-tracking/.

[42] Ken Cor & Gaurav Sood, *Pwned: How Often Are Americans' Online Accounts Breached?*, arXiv (Feb. 18, 2019), https://arxiv.org/pdf/1808.01883; Identity Theft Res. Ctr., 2024 Data Breach Report (Jan. 2025), https://www.idtheftcenter.org/wp-content/uploads/2025/02/ITRC_2024DataBreachReport.pdf.

[43] Erika Harrell, *Just the Stats: Data Breach Notifications and Identity Theft, 2021*, Bureau of Just. Stat. (Jan. 2024), https://bjs.ojp.gov/data-breach-notifications-and-identity-theft-2021.

[44] Madeleine Carlisle, *How the Alleged Outing of a Catholic Priest Shows the Sorry State of Data Privacy in America*, Time (Dec. 11, 2023), https://time.com/6083323/bishop-pillar-grindr-data/.

[45] FRHistS & Christl, *supra* note 38.

[46] EPIC, *Data Broker Harms: Domestic Violence Survivors*, https://epic.org/documents/data-broker-harms-domestic-violence-survivors/.

[47] EPIC, *Data Broker Harms: Domestic Violence Survivors*, https://epic.org/wp-content/uploads/2024/11/Data-Broker-Harms-One-Pager-Domestic-Violence-Survivors.pdf.

2. The Commission Should Institute Provisions from the Vacated Rule, with Adjustments for Efficacy

The harms to consumer choice and privacy merit a response from the FTC. The ACLU agrees with Chairman Ferguson that "Americans are tired of getting signed up for unwanted subscriptions that seem impossible to cancel"[48] and encourages the Commission to follow through on its consideration of proposed rulemaking on this topic.

Existing federal laws and regulations do not sufficiently and completely address these practices. Even the Restore Online Shoppers' Confidence Act (ROSCA), which addresses negative option marketing, is limited to internet transactions; today, digital, physical, on-line, and off-line differentiations can be difficult to make, and many problematic transactions occur at or beyond ROSCA's blurry border. Beyond this, the law arguably introduces a greater degree of burden than the Vacated Rule by providing less guidance for companies, and this ambiguity also means consumers are less able to determine when they encounter related unlawful conduct. As the Commission's Press Release and ANPRM note,[49] harmful negative option practices seem to continue despite dedicated enforcement of ROSCA and other related rules.

The FTC should therefore continue fighting back against practices that deprive Americans of the freedom to choose what happens to their data. The Commission should institute the Vacated Rule, with some adjustments. Below, we provide two sets of recommended adjustments to increase the efficacy of provisions (as compared to the Vacated Rule text) having to do with "dark pattern" prevention and verification during cancellation.

Provisions to Protect Express Informed Consent Should Be More Specific and Enforceable

In drafting a new rule, the FTC should establish concrete, specific provisions around "dark patterns." "Dark patterns"—sometimes also referred to as harmful or coercive choice architecture—are design and choice architecture[50] decisions deployed by hundreds of major

[48] Press Release, FTC, FTC Takes Action Against Uber for Deceptive Billing and Cancellation Practices (Apr. 21, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/04/ftc-takes-action-against-uber-deceptive-billing-cancellation-practices.

[49] Press Release, FTC, FTC Seeks Public Comment in Response to Advance Notice of Proposed Rulemaking Regarding Negative Option Marketing Practices (Mar. 11, 2026), https://www.ftc.gov/news-events/news/press-releases/2026/03/ftc-seeks-public-comment-response-advance-notice-proposed-rulemaking-regarding-negative-option. For instance, in 2018, the Commission brought two cases under section 5 involving negative option plans that did not involve either internet sales or telemarketing. *See FTC* v. *Health Rsch. Labs., LLC,* No. 2:17-cv-00467-JDL, 2020 WL 8679976 (D. Me. 2018); *FTC* v. *Mktg. Architects,* No. 2:18-cv-00050 (D. Me. 2018).

[50] Dan Pilat & Sekoul Krastev, *Choice Architecture*, The Decision Lab, https://thedecisionlab.com/reference-guide/psychology/choice-architecture.

companies[51] that undermine individual choice and often impede the honest disclosure of information. This broad and evolving set of techniques include confusing or strenuous navigation, pre-selected options, or unorthodox interactions that serve to prevent cancellation,[52] manufacture data-related consent,[53] and obscure significant information.[54] Provisions to protect consumers from these methods should therefore be designed in a manner that allows for enforcement.

If the Commission chooses to promulgate a negative option rule, we suggest iterating upon provisions from the Vacated Rule meant to regulate relevant design and choice architecture decisions.

In the Vacated Rule, two provisions[55] were meant to address this issue: First, in the context of informed consent, the Vacated Rule states that sellers must "not include any information that interferes with, detracts from, contradicts, or otherwise undermines the ability of consumers to provide their express informed consent."[56] Second, in the context of "other information" present at disclosure, the text states that "all communications, regardless of media, must not contain any other information that interferes with, detracts from, contradicts, or otherwise undermines the ability of consumers to read, hear, see, or otherwise understand the disclosures required by paragraph (a) of this section."[57]

The Commission declined to directly prohibit dark patterns in the Vacated Rule,[58] taking the perspective that the ban on information that "interferes with, detracts from, contradicts, or otherwise undermines" the ability to consent would prevent relevant dark patterns.

Instead of those approaches, we recommend using more specific language than was proposed originally; some regulators have faced difficulties in identifying violations and enforcing the law when these methods have been defined so broadly.[59] A new rule could instead specifically ban

---

[51] Dark Patterns, *Catalog of Dark Patterns*, https://hallofshame.design/collection/; Deceptive Patterns, *Hall of Shame*, https://www.deceptive.design/hall-of-shame.
[52] Dark Patterns, *Obstruction*, https://hallofshame.design/tag/obstruction/; Ben Sauer (@bensauer.net), BlueSky (Aug. 5, 2025, 4:35 PM), https://bsky.app/profile/bensauer.net/post/3lvokomabxs2t; Press Release, FTC, FTC Takes Action Against Amazon for Enrolling Consumers in Amazon Prime Without Consent and Sabotaging Their Attempts to Cancel (June 21, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-takes-action-against-amazon-enrolling-consumers-amazon-prime-without-consent-sabotaging-their.
[53] Dark Patterns, *Privacy Zuckering*, https://hallofshame.design/tag/privacy-zuckering/; Dark Patterns, *Cookie Wall*, https://hallofshame.design/tag/cookie-wall/; *see generally* Dark Patterns, *supra* note 51.
[54] Deceptive Patterns, *Visual Interference*, https://www.deceptive.design/types/visual-interference.
[55] Negative Option Rule, 89 Fed. Reg. 90476 § VII.B.5 (Nov. 15, 2024), https://www.federalregister.gov/d/2024-25534/p-498; *id.* § VII.B.5(B)(3), https://www.federalregister.gov/d/2024-25534/p-573.
[56] *Id.* § 425.5(a)(2), https://www.federalregister.gov/d/2024-25534/p-1159.
[57] *Id.* § 425.4(b)(3), https://www.federalregister.gov/d/2023-07035/p-268.
[58] *Id.* § VII.B.5(B)(3), https://www.federalregister.gov/d/2024-25534/p-573.
[59] *Cf. NetChoice, LLC v. Bonta*, No. 25-2366, 2026 WL 694471, at *16 (9th Cir. Mar. 12, 2026) (upholding injunction against dark patterns provisions due to vagueness of "materially detrimental" standard); *NetChoice v.*

dark patterns or coercive choice architecture in signup and cancellation flows. The rule could provide for enforcement where a practice meets the specifications below:

1. The pattern is a part, whole, or set of physical, digital, audio, visual, tactile, or otherwise interactive user interface(s) and/or choice architecture;
2. The pattern is obfuscatory, deceptive, unfair, steering, or otherwise interferes with, detracts from, or contradicts express informed consent or choice, as observed through one or more of: (a) any reasonable method of quantitative analysis or testing;[60] (b) any reasonable method of qualitative analysis or testing;[61] (c) expert analysis; (d) any reasonable set of mixed-methods analyses or testing;[62]
3. The deployer, developer, implementer, provider, or other party that exposes the consumer to the dark pattern will benefit in the near- or long-term from resultant changes in consumer consent or choice patterns; and,
4. Consumers are harmed through financial expenditure, data disclosure, or data retention that would not have otherwise occurred, and related loss of time or labor.

Cancellation Verification Asymmetry Should Be More Carefully Regulated

The Commission should be more circumspect in permitting variations among certain elements of companies' cancellation practices than the approach taken in the Vacated Rule. In the discussion of cancellation standards in the Vacated Rule, the Commission indicated an allowance for some degree of deviation from cancellation being as least as simple as consent given the "verification, authentication, or confirmation procedures" sometimes needed for cancellation.[63] The limit of this flexibility in the discussion was "unreasonable asymmetry."[64]

Brown, No. CV RDB-25-0322, 2025 WL 3267786, at *19 (D. Md. Nov. 24, 2025) ("best interests of the child" standard incorporated in dark patterns provision unconstitutionally vague).

[60] Kate Moran, *Quantitative User-Research Methodologies: An Overview*, NNGroup (Apr. 22, 2018), https://www.nngroup.com/articles/quantitative-user-research-methods/.

[61] Kate Moran, *Qualitative Usability Testing: Study Guide*, NNGroup (July 24, 2024), https://www.nngroup.com/articles/qual-usability-testing-study-guide/.

[62] The Commission has previously ordered the preservation of "any market, behavioral, or psychological research, or user, customer, or usability testing, including any A/B or multivariate testing, copy testing, surveys, focus groups, interviews, clickstream analysis, eye or mouse tracking studies, heat maps, or session replays or recordings" to "help prevent further use of deceptive dark patterns." Press Release, FTC, FTC Takes Action to Stop Credit Karma From Tricking Consumers With Allegedly False "Pre-Approved" Credit Offers (Sept. 1, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-takes-action-stop-credit-karma-tricking-consumers-allegedly-false-pre-approved-credit-offers.

[63] Negative Option Rule, 89 Fed. Reg. 90476 § VII.B.6(a) (Nov. 15, 2024), https://www.federalregister.gov/d/2024-25534/p-613.

[64] *Id.*

Certain products and services, such as home alarm systems, have an understandable need to authenticate their customers before cancellation. However, the text of the Vacated Rule could be interpreted as providing an allowance for deviation from the "as-simple-as" standard when verification is mandated to cancel, reflected by an absence of particular provisions about verification. Such a gap could in turn create a degree of ambiguity that allows bad actors to prevent cancellation, enables these actors to gather data in a manipulative way, and increases compliance burdens for small actors.

We therefore suggest the following:

- The Commission should create and maintain a standard that requires proportional and privacy-preserving reasoning for each piece of information or proof requested for cancellation beyond what would be requested at signup.

  The standard should urge data minimization and data security best practices, requesting a balance of only the least sensitive information, the smallest volume of information, and the least individually identifying information (e.g., zip code instead of home address) that is reasonably necessary.

- Given the rarity of the need for verification procedures that would create distinct differences in information provided between signup and cancellation, any diversion from the expectations of the "as simple as" cancellation standard merits scrutiny. A potential rule should therefore require companies that deploy such procedures to create, and either submit or retain, simple summaries of what they request, why, and how it compares to the FTC's standard described above.

  Given the volume of companies impacted by a potential negative option rule, such a process could encourage good practices and increase the likelihood of effective enforcement without generating any additional burden for most actors.

- Any negative option rule should explicitly prevent any harvesting of information provided by consumers during cancellation other than as required by law.

The ACLU greatly appreciates the focus of Chairman Ferguson and the entire FTC on negative option practices, and we hope that this effort can bolster privacy and choice for all Americans. We urge the Commission to incorporate our recommendations to increase the efficacy of protections

for express informed consent and “as easy as” cancellation. If you have any questions about this legislation, please contact Cody Venzke at cvenzke@aclu.org or Varun Gadh at vgadh@aclu.org. Thank you again for your work on this matter.