Target(ed) Advertising

Derek E. Bambauer[*]

Targeted advertising — using data about consumers to customize the ads they receive — is deeply controversial. It also creates a regulatory quandary. Targeted ads generate more money than untargeted ones for apps and online platforms. Apps and platforms depend on this revenue stream to offer free services to users, if not for their financial viability altogether. However, targeted advertising also generates significant privacy risks and consumer resentment. Despite sustained attention to this issue, neither legal scholars nor policymakers have crafted interventions that address both concerns, and existing regulatory regimes for targeted advertising have critical gaps.

This Article makes three key contributions to the targeted advertising literature. First, it rigorously interrogates the empirical evidence on the effectiveness of the practice, concluding that targeted ads generate important benefits for firms, but mixed effects for society. Next, it evaluates the risks and harms of these ads and maps them onto existing regulatory regimes to identify gaps. Finally, it elucidates a co-regulatory reform proposal that combines industry expertise with oversight by the Federal Trade Commission to address invasive data collection techniques, insecure data storage, and problematic transactions in consumer data. The proposal closes regulatory loopholes, reduces information asymmetry for enforcement in a fast-changing industry, and offers a pragmatic path to implementation.

 Irving Cypen, Professor of Law, University of Florida Levin College of Law. I owe thanks for helpful suggestions and discussion to BJ Ard, Jane Bambauer, Gus Hurwitz, Gavin Milczarek-Desai, Shefali Milczarek-Desai, Thinh Nguyen, Dave Schwartz, Kristian Stout, and the participants at two workshops at the Governance & Technology Center at the University of Nebraska. I am grateful to Taylor Col, Will Liu, and Javier Lopez-Nieto for expert research assistance. This project was supported by a grant from the International Center for Law & Economics; all views in this paper are entirely my own. I welcome comments at <bambauer@law.ufl.edu>.

TABLE OF CONTENTS

INTRODUCTION

Targeted advertising has suddenly become a target, and privacy issues are the bull's-eye at the center. Consider two recent examples.

First, the Federal Trade Commission ("FTC"), in its role as the leading privacy regulator in the United States, has begun to scrutinize targeted ads. For example, the online mental health counseling firm BetterHelp collected information from millions of consumers — including their health histories, e-mail addresses, and intake questionnaires — to match users seeking therapy with treatment providers.[1] The company repeatedly pressured consumers to disclose this information on its Web sites, reassuring them at each step that the information would be kept private[2] and would not be used for advertising.[3] However, BetterHelp used these consumers' sensitive data to target ads to users of Facebook, Pinterest, Snapchat, and other social media platforms, including by transferring the data to these companies.[4] Even sharing consumers' e-mail addresses constituted a significant privacy violation: BetterHelp users were, by definition, people who sought assistance with mental health issues[5] and who continued to suffer from significant, unwarranted social stigma.[6] BetterHealth settled with the FTC,[7] but its targeted advertising practices are hardly unique.[8]

---

[1] Complaint at 1-2, *In re* BetterHelp Inc., (2023) (No. C-4796).

[2] *See id.* at 4-9.

[3] *Id.* at 2.

[4] *Id.*

[5] *Id.* at 1-2.

[6] *See* Claire Sontheimer & Michael R. Ulrich, *Addressing Stigma and False Beliefs About Mental Health: A New Direction for Mental Health Parity Advocacy*, 31 ANNALS HEALTH L. & LIFE SCIS. 101, 107-10 (2022).

[7] Decision and Order, *In re* BetterHelp, Inc., (2023) (No. C-4796).

[8] *See* Complaint at 8-9, United States v. Easy Healthcare Corp., (2023) (No. 1:23-cv-3107) (sharing consumer health information, including about fertility, with third parties for advertising purposes in contravention of promises to the contrary).

Second, individual plaintiffs have also challenged the misuse of targeted ads. In June 2023, the U.S. Court of Appeals for the Ninth Circuit issued its decision in a class action lawsuit against Facebook over targeted advertising.[9] Rosemarie Vargas, the lead plaintiff, alleged that Facebook discriminated against her because she was a "single parent [and a] disabled female of Hispanic descent."[10] Formally, the Ninth Circuit's legal analysis concentrated on technical questions such as standing and whether Facebook was protected under 47 U.S.C. § 230 (popularly known as "Section 230").[11]

The heart of the case, though, was the advertising machine that powers Facebook's massive social networking platform.[12] Facebook's Ad Platform enables advertisers to determine which users receive an ad based upon variables including sex, age, and location.[13] Facebook requires users to disclose some of this data to use the service; the firm can infer additional variables by employing machine learning and other algorithmic techniques, popularly known as "artificial intelligence."[14] Facebook's protestations that it was the advertisers, not the platform, who were engaged in any unlawful conduct left the Ninth Circuit

[9] *See* Vargas v. Facebook, Inc., No. 21-16499, 2023 WL 4145434, at *1-2 (9th Cir. June 23, 2023).

[10] *Id.* at 2.

[11] *See* Derek E. Bambauer, *What Does the Day After Section 230 Reform Look Like?*, BROOKINGS (Jan. 22, 2021), https://www.brookings.edu/articles/what-does-the-day-after-section-230-reform-look-like/ [https://perma.cc/7XS2-BBJC].

[12] *See* Eric Goldman, *Uh-Oh, the Ninth Circuit is Messing Again With its Roommates Ruling* — Vargas v. Facebook, TECH. & MKTG. L. BLOG (June 26, 2023), https://blog.ericgoldman.org/archives/2023/06/uh-oh-the-ninth-circuit-is-messing-again-with-its-roommates-ruling-vargas-v-facebook.htm [https://perma.cc/U264-ZAK5].

[13] *See* Linda Morris & Olga Akselrod, *Holding Facebook Accountable for Digital Redlining*, ACLU (Jan. 27, 2022), https://www.aclu.org/news/privacy-technology/holding-facebook-accountable-for-digital-redlining [https://perma.cc/2XYT-ZAJC].

[14] *See* Tony Phillips, *One to Watch: Has the Ninth Circuit Turned on Section 230?*, PILLSBURY (July 20, 2023), https://www.pillsburylaw.com/en/news-and-insights/ninth-circuit-section-230.html#:~:text=Although%20the%20trial%20court%20denied,the%20specific%20editing%20or%20selection [https://perma.cc/JSL3-K8W6] (noting that "[m]ost of the attributes used to target ads were not based on information expressly provided by individual users about themselves, but rather were determined by the platform's algorithm"). *See generally* Cole Stryker & Eda Kavlakoglu, *What Is Artificial Intelligence?*, IBM, https://www.ibm.com/topics/artificial-intelligence (last visited Jan. 18, 2024) [https://perma.cc/5N67-7X7H] (providing an overview of definitions).

unmoved. The court reversed and remanded the district court's initial dismissal of the case.[15] Facebook thus faces the risk that its only significant revenue source — targeted advertising — could be a serious legal liability.[16] Regardless of the case's outcome, larger questions about whether advertisers ought to be able to choose who sees commercials based on consumer data will persist.[17]

These two examples are individual battles in the escalating wars over regulation of targeted advertising. There is a growing consensus among legal scholars, and increasingly among policymakers, that more oversight and constraints on ads are badly needed — although different commentators advance starkly different reasons for reforms.[18] In 2022 and 2023, targeted advertising rocketed to the top of the political

[15] Vargas v. Facebook, Inc., No. 21-16499, 2023 WL 4145434, at *1-2 (9th Cir. June 23, 2023).

[16] *See* Matthew Johnston, *How Does Facebook (Meta) Make Money?*, INVESTOPEDIA, https://www.investopedia.com/ask/answers/120114/how-does-facebook-fb-make-money.asp#:~:text=Meta%20Platforms%20(META)%2C%20the,its%20various%20social%20media%20platforms (last visited Jan. 10, 2023) [https://perma.cc/929C-2JLH] (disclosing that Facebook earns 98% of revenue from advertising).

[17] For example, could a firm use targeted advertising to recruit female candidates in fields — like computer science — where they are underrepresented? *See* Eitan Frachtenberg & Rhody D. Kaner, *Underrepresentation of Women in Computer Systems Research*, 17 PLOS ONE (Apr. 6, 2022), https://doi.org/10.1371/journal.pone.0266439 [https://perma.cc/T337-PVKG]. Or, could such a firm use targeted advertising to overcome historical discrimination against minority communities? *See* Mark Bulik, *1854: No Irish Need Apply*, N.Y. TIMES (Sept. 8, 2015), https://www.nytimes.com/2015/09/08/insider/1854-no-irish-need-apply.html; Dara Lind, *Why Historians are Fighting About "No Irish Need Apply" Signs — and Why it Matters*, VOX, https://www.vox.com/2015/3/17/8227175/st-patricks-irish-immigrant-history (last updated Aug. 4, 2015, 9:30 AM) [https://perma.cc/PNJ5-PLP2]. *But see* Richard Jensen, *"No Irish Need Apply": A Myth of Victimization*, 36 J. SOC. HIST. 405, 405 (2002).

[18] *See* Oren Bar-Gill, Cass R. Sunstein & Inbal Talgam-Cohen, *Algorithmic Harm in Consumer Markets*, 15 J. LEGAL ANALYSIS 1, 23-24 (2023); Neil M. Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961, 1003-12 (2021); John A. Rothchild, *Sham Choice: How the Current Privacy Regime Fails Us, and How to Fix It*, 92 UMKC L. REV. 169, 196-98 (2023); Noelle Wilson & Amanda Reid, *Data Controllers as Data Fiduciaries: Theory, Definitions & Burdens of Proof*, 95 U. COLO. L. REV. 175, 210-12 (2024); Abby K. Wood & Ann M. Ravel, *Fool Me Once: Regulating 'Fake News' and Other Online Advertising*, 91 S. CAL. L. REV. 1223, 1253-73 (2018).

agenda.[19] Dozens of bills were proposed in both houses of Congress;[20] state attorneys general brought lawsuits based upon unfair competition and antitrust statutes;[21] and foreign regulators, such as data protection authorities in the European Union, had an increasingly weighty effect on the advertising shown to American consumers.[22] At the federal level, Congress was unable to pass legislation that would further regulate targeted advertising, and the looming 2024 election makes it unlikely that legislative reform will be adopted this year.[23] The litigation over targeted advertising will take years to resolve. Thus, regardless of the outcome in November 2024, targeted advertising will remain a top

[19] *See, e.g.*, Scott Clark, *Will Targeted Advertising Survive Privacy Legislation?*, CMSWIRE (Sept. 15, 2023), https://www.cmswire.com/digital-marketing/will-targeted-advertising-survive-privacy-legislation/ [https://perma.cc/KA69-ZWCU]; Cecilia Kang & David McCabe, *Efforts to Rein in Big Tech May Be Running Out of Time*, N.Y. TIMES (Jan. 20, 2022), https://www.nytimes.com/2022/01/20/technology/big-tech-senate-bill.html; Natasha Singer, *This Ad's for You (Not Your Neighbor)*, N.Y. TIMES (Sept. 20, 2022), https://www.nytimes.com/2022/09/15/business/custom-political-ads.html; Natasha Singer, *U.S. Regulators Propose New Online Privacy Safeguards for Children*, N.Y. TIMES (Dec. 20, 2023), https://www.nytimes.com/2023/12/20/technology/ftc-regulation-children-online-privacy.html.

[20] *See, e.g.*, Advertising Middlemen Endangering Rigorous Internet Competition Accountability (AMERICA) Act, S. 1073, 118th Cong. (2023); Children and Teens' Online Privacy Protection Act, S. 1418, 118th Cong. (2023); American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022); Banning Surveillance Advertising Act, H.R. 6416, 117th Cong. (2022).

[21] *See* Press Release, New York State Attorney General, Attorney General James Sues Google for Monopolies in Digital Advertising (Jan. 24, 2023), https://ag.ny.gov/press-release/2023/attorney-general-james-sues-google-monopolies-digital-advertising [https://perma.cc/BB86-UJBB]; Press Release, Attorney General of Texas, Paxton Defeats Google's Efforts to Avoid Transfer of Landmark Antitrust Case Back to Texas (Oct. 4, 2023), https://www.texasattorneygeneral.gov/news/releases/paxton-defeats-googles-efforts-avoid-transfer-landmark-antitrust-case-back-texas [https://perma.cc/UDE9-H7DE].

[22] *See* Gwladys Fouche, *Facebook Owner Meta Faces EU Ban on Targeted Advertising*, REUTERS, https://www.reuters.com/technology/facebook-owner-faces-eu-ban-targeted-advertising-norway-says-2023-11-01/ (last updated Nov. 1, 2023, 10:02 AM).

[23] *See The Anti-Predictions: Here's What Won't Happen in Advertising in 2024*, DIGIDAY (Jan. 2, 2024), https://digiday.com/marketing/the-anti-predictions-heres-what-wont-happen-in-advertising-in-2024/ [https://perma.cc/83UV-N8TP] [hereinafter *Anti-Predictions*].

policy priority in the coming years.[24] Moreover, there are trends that indicate the issues with targeted advertising will worsen soon, making reform critical.[25]

Targeted advertising is a critical, hotly contested policy issue for at least four reasons. First, technology firms such as social media platforms depend upon it for most, if not nearly all, of their revenue.[26] Limits on targeted advertising would have significant adverse financial effects for these companies, who oppose them vigorously.[27] Second, American consumers hold mixed and sometimes contradictory views about personalized advertising. Users hate untargeted ads and find some data collection practices disturbing; however, they want online services such as social media to be free in monetary terms, which means tolerating advertising as an exchange.[28] Third, the technology that makes targeted advertising possible changes constantly.[29] It is difficult

[24] *Id.*

[25] *See infra* CONCLUSION.

[26] *See, e.g.*, Megan Graham & Jennifer Elias, *How Google's $150 Billion Advertising Business Works*, CNBC, https://www.cnbc.com/2021/05/18/how-does-google-make-money-advertising-business-breakdown-.html (last updated Oct. 13, 2021) [https://perma.cc/XBM6-BK7Y] (noting over 80% of Alphabet's revenue is from advertising; Alphabet is the parent company of Google); Johnston, *supra* note 16.

[27] *See* Emily Birnbaum, *Big Tech Divided and Conquered to Block Key Bipartisan Bills*, BLOOMBERG NEWS (Dec. 20, 2022), https://www.bloomberg.com/news/articles/2022-12-20/big-tech-divided-and-conquered-to-block-key-bipartisan-bills; Eric Cortellessa, *Schumer Kills Bills Big Tech Feared Most, But Boosts Budgets of Agencies Targeting Them*, TIME, https://time.com/6243256/schumer-kills-antitrust-big-tech-bills/ (last updated Dec. 22, 2022, 3:42 PM) [https://perma.cc/NQN9-T5MX]; Makena Kelly, *Congress Blew Its Last Chance to Curb Big Tech's Power*, VERGE (Dec. 20, 2022, 6:18 AM), https://www.theverge.com/2022/12/20/23517807/big-tech-antitrust-bills-congress-omnibus [https://perma.cc/QP2Y-YT6D].

[28] *See* Neil Cumins, *Invasion of Privacy? What Consumers Think of Personalized Online Ads*, BUS. NEWS DAILY, https://www.businessnewsdaily.com/4632-online-shoppers-personal-ads.html# (last updated Oct. 23, 2023) [https://perma.cc/CQJ7-VPY2]; Leslie K. John, Tami Kim, & Kate Barasz, *Ads That Don't Overstep*, HARV. BUS. REV. (Jan.–Feb. 2018), https://hbr.org/2018/01/ads-that-dont-overstep [https://perma.cc/N6VH-68EB]. *See generally* Stephen J. Hoch & George F. Loewenstein, *Time-Inconsistent Preferences and Consumer Self-Control*, 17 J. CONSUMER RSCH. 491 (1991), https://doi.org/10.1086/208573 [https://perma.cc/S43G-G2DH].

[29] *See* Seb Joseph, *Nine Questions to Consider as Google Starts its Move Away from Third-Party Cookies*, DIGIDAY (Jan. 4, 2024), https://digiday.com/marketing/nine-questions-to-

for advertisers to remain current with the technological state of play, and it is far more difficult for regulators to do so. Rules that govern advertising are likely to become outmoded quickly. Finally, targeted advertising raises significant privacy concerns that sharpen as personalized content moves beyond commercial topics and involves contested political issues.[30] This Article critically evaluates each of these issues and their implications for proposals to reform oversight of online advertising.

To date, the scholarly and policy debate over targeted advertising has been a clash of extremes. On one side, information technology companies — especially platforms — emphasize that they can only offer services to consumers at zero monetary cost by earning revenues from advertising.[31] For platforms, targeted advertising is more lucrative than untargeted advertising and, potentially, more desirable to consumers.[32] Therefore, advertisers prefer the status quo. On the other side, commentators decry the risks of targeted advertising, from gathering sensitive data to inferring information about consumers that they would prefer to keep confidential.[33] Fears about personalized advertising have grown with the increasing prominence of machine learning techniques,

consider-as-google-starts-its-move-away-from-third-party-cookies/ [https://perma.cc/8WDW-CJXR].

[30] *See* Katherine J. Strandburg, *Free Fall: The Online Market's Consumer Preference Disconnect*, 2013 U. CHI. LEGAL F. 95, 164-65; *infra* Part III.

[31] *See* Kendra Barnett, *New US Bill Aims to Kill Targeted Advertising: The Industry Reacts*, DRUM (Jan. 20, 2022), https://www.thedrum.com/news/2022/01/20/new-us-bill-aims-kill-targeted-advertising-the-industry-reacts [https://perma.cc/VKE7-49J3]; Paul Karp, *Meta Warns Australia's Plan to Limit Targeted Ads Could Push Free Platforms Towards Subscription Fees*, GUARDIAN (May 17, 2023), https://www.theguardian.com/technology/2023/may/18/meta-warns-australia-platforms-facebook-instagram-harmed-by-limiting-targeted-ads [https://perma.cc/9U66-8T7X].

[32] *See* Avi Goldfarb & Catherine E. Tucker, *Privacy Regulation and Online Advertising*, 57 MGMT. SCI. 57, 67-68 (2011), https://doi.org/10.1287/mnsc.1100.1246; Christopher A. Summers, Robert W. Smith & Rebecca Walker Reczek, *An Audience of One: Behaviorally Targeted Ads as Implied Social Labels*, 43 J. CONSUMER RSCH. 156, 171-72 (2016).

[33] *See* Bennett Cyphers & Adam Schwartz, *Ban Online Behavioral Advertising*, ELEC. FRONTIER FOUND. (Mar. 21, 2022), https://www.eff.org/deeplinks/2022/03/ban-online-behavioral-advertising [https://perma.cc/3KVA-SH4E]; David Dayen, *Ban Targeted Advertising*, NEW REPUBLIC (Apr. 10, 2018), https://newrepublic.com/article/147887/ban-targeted-advertising-facebook-google [https://perma.cc/3UQK-4BUJ].

popularly termed "artificial intelligence," that analyze vast troves of data to generate inferences about consumers.[34] Concomitantly, many scholarly and legislative proposals would significantly limit, if not fully ban, targeted ads.[35]

This polarized discourse elides some hard truths about targeted advertising. First, major regulatory changes are unlikely to occur soon because of political divisions in the elected branches of the federal government.[36] While the 2024 election might provide one party with both the presidency and control of Congress, there are also intraparty divisions over online advertising.[37] Second, many popular online services are free to users because they are funded via advertising. Consumers are familiar with this model and prefer it to fee-for-service pricing.[38] Reforms that require customers to pay with dollars rather than data are unlikely to be politically viable. Third, regulatory proposals that restrict use of sensitive data for advertising are unlikely to succeed, both because sensitive information can be readily inferred from non-sensitive data,[39] and because some rationales for using sensitive data are

---

[34] *See* Tom Huddleston Jr., *You're Right to Be Scared of A.I., Says Ivy League Expert and White House Advisor — These 5 Guardrails Can Protect 'Against Harm,'* CNBC (May 6, 2023, 9:00 AM), https://www.cnbc.com/2023/05/06/youre-right-to-be-scared-of-ai-white-house-advisor-ivy-league-expert.html [https://perma.cc/6CK2-P9Z8].

[35] *See, e.g.*, American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022); Banning Surveillance Advertising Act of 2022, H.R. 6416, 117th Cong. (2022); Mason Marks, *Emergent Medical Data: Health Information Inferred by Artificial Intelligence*, 11 U.C. IRVINE L. REV. 995, 1064 (2021); Anuj Puri, *The Right to Attentional Privacy*, 48 RUTGERS L. REC. 206, 214 (2021).

[36] *See Anti-Predictions*, *supra* note 23.

[37] *See* Alfred Ng, *Pelosi Expresses Reservations About Bipartisan Privacy Bill*, POLITICO, https://www.politico.com/news/2022/09/01/speaker-pelosi-reservations-privacy-bill-00054559 (last updated Sept. 1, 2022, 5:06 PM).

[38] *See* Peter Suciu, *Will Users Subscribe to a Tiered Social Media Service?*, FORBES (Oct. 9, 2023, 3:30 PM), https://www.forbes.com/sites/petersuciu/2023/10/09/will-users-subscribe-to-a-tiered-social-media-service/?sh=15d1397a14eb [https://perma.cc/BW2S-YV2B].

[39] *See* Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1138-40 (2015); Till Speicher, Muhammad Ali, Giridhari Venkatadri, Filipe Nunes Ribeiro, George Arvanitakis, Fabrício Benevenuto, Krishna P. Gummadi, Patrick Loiseau & Alan Mislove, *Potential for Discrimination in Online Targeted Advertising*, 81 PROC. MACH. LEARNING RSCH. 1, 11 (2018) (demonstrating that "malicious advertisers can exploit Facebook's

generally unobjectionable[40] Fourth, Americans have significant, widely shared concerns about personalized advertising; the regulatory status quo will face increasing political pressure for change.[41] Finally, much of the scholarly and policy debate has been largely devoid of empirical data on the effects of targeted advertising — data that is essential to crafting effective reform that mitigates privacy issues without unnecessarily damaging popular Internet services.

This Article offers an alternative to the all-or-nothing approaches that characterize the current debate about targeted ads — one that is grounded in empirical data. It interrogates the assumptions of both sides, examining studies on the efficacy of targeted advertising and analyzing the harms it can cause. This Article takes account of the complex regulatory landscape: targeted advertising creates difficult hurdles for meaningful governance because it mixes rapidly changing technology[42] with a complex ecosystem of institutions and actors.[43] Regulators always struggle with information asymmetries; it is particularly hard to gain and maintain expertise when the industry at issue is constantly in flux.[44] To overcome these challenges, this Article proposes a novel intervention that employs a co-regulatory model, rare in the American legal system, that blends public oversight and enforcement from the Federal Trade Commission ("FTC") with private industry expertise. Such a model mitigates privacy harms from targeted

suggestions to discover new facially neutral free-form attributes that allow extremely biased targeting").

[40] *See, e.g.*, Algorithmic Justice and Online Platform Transparency Act, H.R. 3611, 117th Cong. § 6(g)(2) (2021) (allowing platforms to process personal information for "advertising, marketing, or soliciting economic opportunities . . . to underrepresented populations").

[41] *See* John, Kim & Barasz, *supra* note 28.

[42] *See* Jonathan Vanian, *How the Generative A.I. Boom Could Forever Change Online Advertising*, CNBC, https://www.cnbc.com/2023/07/08/how-the-generative-ai-boom-could-forever-change-online-advertising.html (last updated July 12, 2023) [https://perma.cc/QH6U-9LCE].

[43] *See* Stella Morrison, *How Technology Is Changing Online Advertising*, BUSINESS.COM, https://www.business.com/articles/how-technology-is-changing-online-advertising/ (last updated Apr. 15, 2023) [https://perma.cc/6RGZ-UUNL].

[44] *See* Cary Coglianese, Richard Zeckhauser & Edward Parson, *Seeking Truth for Power: Informational Strategy and Regulatory Policymaking*, 89 MINN. L. REV. 277, 297-300 (2004).

advertising while maintaining the consumer benefits the practice can offer.[45]

This Article makes three key contributions to the scholarly literature on advertising. First, it brings rigor to the debate on whether targeted advertising is necessary for platforms by examining data about its effects rather than relying on theory. Second, this Article maps a set of gaps in the current governance regime, linking them to harms that personalized ads can cause. It contends that legal reform should concentrate on transactions in personally identifiable information, invasive data collection techniques, and insecure data storage. Finally, this Article offers a policy intervention that is simultaneously more effective and more politically palatable than other alternatives — and sets forth a mechanism for evaluating its success if adopted.

This Article proceeds in five Parts. Part I evaluates empirical data on the effectiveness of targeted ads relative to their untargeted counterparts. Part II examines the rapidly shifting technological landscape with which regulators and regulated alike must contend. Then, Part III evaluates the harms, both actual and potential, that drive demands for greater regulation of targeted advertising, with particular focus on concerns grounded in privacy. Next, Part IV assesses existing legal regimes that govern targeted advertising. Finally, Part V proposes a carefully crafted intervention based on co-regulation that can mitigate these unaddressed harms and adapt to the unceasing changes in the advertising industry. This Article concludes by considering the forces that will continue to make Internet advertising both targeted and a target in years to come.

I. THE MONEY

Targeted advertising works. That conclusion, which is robustly supported by empirical evidence, is plainly good for platforms and advertisers. Users benefit from attractive online services that are free in

[45] *See* Cameron F. Kerry & Mishaela Robison, *Rulemaking in Privacy Legislation Can Help Dial in Ad Regulation*, BROOKINGS (Dec. 5, 2022), https://www.brookings.edu/articles/rulemaking-in-privacy-legislation-can-help-dial-in-ad-regulation/ [https://perma.cc/6EPX-BWSL] (arguing Congress should enable the FTC to engage in rulemaking for online advertising due to its expertise, the rapidly changing technologies involved, and the FTC's ability to garner broad input on proposals).

monetary terms;[46] however, there is some experimental evidence to suggest that targeted advertising can worsen consumer purchasing choices.[47] Large majorities of survey respondents consistently object to targeted advertising, although their online behavior indicates that their revealed preferences differ strongly from their expressed ones. This Part evaluates the empirical evidence for customized ads.

A. Advertising Expenditures

Online advertising is a lucrative business. A study by the consulting firm PwC for the Internet Advertising Bureau found that U.S. online ad industry revenues totaled almost $210 billion in 2022, a 10.8% increase over the prior year.[48] The worldwide market was estimated at approximately $567 billion in 2022 and at roughly $626 billion in 2023.[49] Early results and analyst projections suggested that 2023 had slower growth due to factors such as inflation, economic uncertainty, and privacy regulation.[50] Advertising revenue from search engines was the largest component of U.S. Internet advertising revenue in 2022, at $84.4 billion (40.2%).[51]

---

[46] *See* Pinar Akman, *A Web of Paradoxes: Empirical Evidence on Online Platform Users and Implications for Competition and Regulation in Digital Markets*, 16 VA. L. & BUS. REV. 217, 247-51 (2022).

[47] *See* Eduardo Abraham Schnadower Mustri, Idris Adjerid & Alessandro Acquisti, *Behavioral Advertising and Consumer Welfare: An Empirical Investigation* 1, 14 (Mar. 23, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4398428 [https://perma.cc/FV5R-6TG6].

[48] PWC, INTERNET ADVERTISING REVENUE REPORT: FULL-YEAR 2022 RESULTS 5-6 (2023) (on file with author).

[49] *See* Sara Lebow, *Worldwide Digital Ad Spend Will Top $600 Billion This Year*, EMARKETER (Jan. 31, 2023), https://www.insiderintelligence.com/content/worldwide-digital-ad-spend-will-top-600-billion-this-year [https://perma.cc/T7XF-37L5].

[50] *See* Vidhi Choudhary, *The Digital Ad Market Is in a Slump*, MOD. RETAIL (Feb. 7, 2023), https://www.modernretail.co/technology/the-digital-ad-market-is-in-a-slump/ [https://perma.cc/A6GZ-V5QP] (reporting drop in advertising revenue in the fourth quarter of 2022 of 3.6% for Google and 4.2% for Meta).

[51] Danny Goodwin, *U.S. Search Ad Revenue Hit a Record $84.4 Billion in 2022*, SEARCH ENGINE LAND (Apr. 12, 2023, 11:21 PM), https://searchengineland.com/search-ad-revenue-84-billion-395575 [https://perma.cc/SY44-D6ZR].

Organizations invest significant sums in targeted advertising, but there is limited data on both absolute expenditures and growth rates.[52] There is a general consensus that firms are increasing their spending on customized advertising.[53] Certain major platforms, especially Facebook, derive nearly all of their revenue from targeted advertising.[54] In addition, terminology may be a barrier to better aggregated data: advertisers distinguish between contextual advertising, which is driven by the content that the user is accessing, and behavioral advertising, which is generated based upon the user's prior activity.[55] Some firms also employ a third term, "psychographic targeting," to denote advertising that is based upon a user's offline characteristics such as hobbies or lifestyle.[56] Advertising methods may blend one or more of these approaches, and a 2016 study based on automobile advertising found that combining behavioral targeting and contextual targeting was more effective than any of the strategies alone.[57] Organizations are thus spending more of their growing advertising budgets on targeted advertising, but it is difficult to quantify these investments with precision.

B. Theory and Data

Historically, research on targeted advertising has concentrated heavily on theory. The results have been mostly positive for the technique. For example, economic modeling of publisher revenues from

---

[52] *Cf.* Strandburg, *supra* note 30, at 100 (discussing dearth of reliable data generally for targeted advertising).

[53] *See* J.G. Navarro, *Marketing Personalization in the United States — Statistics & Facts*, STATISTA (Dec. 18, 2023), https://www.statista.com/topics/10058/marketing-personalization-in-the-united-states/ [https://perma.cc/R8XQ-RMZK].

[54] *See* Johnston, *supra* note 16.

[55] *See* Zack Rosenberg, *Contextual Versus Behavioral Advertising: Which Is Which?*, ASS'N OF NAT'L ADVERTISERS (July 12, 2022), https://www.ana.net/miccontent/show/id/ii-2022-07-context-behavorial-advertising [https://perma.cc/R37R-8NJM].

[56] *See* David Simutis, *Contextual Advertising: What It Is, How It Works, and Why to Use It*, PEER39 (Jul. 8, 2022), https://www.peer39.com/blog/contextual-advertising [https://perma.cc/L6VC-7ZPE].

[57] *See* Xianghua Lu, Xia Zhao & Ling Xue, *Is Combining Contextual and Behavioral Targeting Strategies Effective in Online Advertising?*, 7 ACM TRANSACTIONS ON MGMT. INFO. SYS. 1, 15 (2016).

behavioral targeting shows that this advertising technique can be either a boon or a bane for sites depending upon factors including the level of competition among advertisers and the degree to which users are more likely to click on targeted ads.[58] The model also suggested implications for competition policy: its results found that smaller advertisers would benefit from behavioral targeting, while dominant advertisers might benefit from a prohibition on such advertising because it would allow them to capture a larger segment of users.[59] Overall, the model predicts that behavioral advertising leads to a net increase in social welfare.[60] Similarly, a 2005 study showed with its model that targeted advertising can increase firms' profits even if those firms cannot engage in price discrimination, and that under competitive conditions, targeted advertising may be a more valuable tool than such price discrimination.[61] Another 2005 study modeled customized advertising with a single, monopolistic content distributor, finding that even under conditions where collusion among producers undercuts price competition, consumer welfare is nonetheless increased by targeted ads.[62]

More recently, empirical studies have begun to employ data from consumer transactions to evaluate targeted advertising. Most prominently, the European Union's privacy legislation has created a natural experiment to measure the relative benefits of targeted versus untargeted ads. The European Union ("EU") places strict limits on the collection and use of consumer data in advertising.[63] Thus, ads displayed online to EU users, from EU-based sites, are almost always untargeted, in contrast to ads displayed online to users from non-EU sites.[64] A 2011

[58] *See* Jianqing Chen & Jan Stallaert, *An Economic Analysis of Online Advertising Using Behavioral Targeting*, 38 MIS Q. 429, 447 (2014).

[59] *Id.*

[60] *Id.* at 431.

[61] Ganesh Iyer, David Soberman & J. Miguel Villas-Boas, *The Targeting of Advertising*, 24 MKTG. SCI. 461, 473 (2005).

[62] Esther Gal-Or & Mordechai Gal-Or, *Customized Advertising via a Common Media Distributor*, 24 MKTG. SCI. 241, 250 (2005).

[63] *See* Lex Zard & Alan M. Sears, *Targeted Advertising and Consumer Protection Law in the European Union*, 56 VAND. J. TRANSNAT'L L. 799, 821-22 (2023).

[64] Some non-EU sites may observe EU rules on behavioral advertising to reduce legal risk from intervention by EU data protection authorities. *See generally* Mark

study found that the EU adoption of restrictions on targeted advertising meant that "advertising effectiveness decreased on average by around 65% in Europe relative to the rest of the world."[65] The study carefully controlled for differences in advertising preferences between EU and non-EU consumers by assessing how each group reacted to EU versus non-EU advertising.[66] When EU consumers visited non-EU sites, there was no reduction in advertising effectiveness. When non-EU users visited EU sites, there was such a reduction.[67] To maintain their current level of effectiveness, advertisers would need to spend almost three times as much on advertising for the same impact.[68]

Similarly, smaller-scale studies demonstrate that targeted Internet ads cost more to place than untargeted ones — but they are worth it to advertisers, and likely to consumers as well.[69] A 2009 study that analyzed log files from a search engine found that the click-through rate for users increased by as much as 670% when behavioral targeting techniques were used to select which ads to display.[70] A 2010 study evaluating data from twelve ad networks found that targeted ads cost 2.68 times as much, on average, as targeted ones — and that the increased price benefited advertisers since conversion rates (the share

MacCarthy, *The European Data Protection Board (EDPB) Goes After Tech's Personalized Ad Business Model*, BROOKINGS (Feb. 1, 2023), https://www.brookings.edu/articles/the-european-data-protection-board-goes-after-techs-personalized-ad-business-model/ [https://perma.cc/N8ND-N2MZ].

[65] Goldfarb & Tucker, *supra* note 32, at 58.

[66] *Id.*

[67] *Id.*

[68] *See id.* at 68.

[69] *See generally* YAN LAU, FED. TRADE COMM., ECONOMIC ISSUES: A BRIEF PRIMER ON THE ECONOMICS OF TARGETED ADVERTISING 5-7 (2020), https://www.ftc.gov/system/files/documents/reports/brief-primer-economics-targeted-advertising/economic_issues_paper_-_economics_of_targeted_advertising.pdf [https://perma.cc/SQN7-HFP8]; Jiwoong Shin & Jungju Yu, *Targeted Advertising and Consumer Inference*, 40 MKTG. SCI. 900, 900 (2021).

[70] Jun Yan, Ning Liu, Gang Wang, Wen Zhang, Yun Jiang & Zheng Chen, *How Much Can Behavioral Targeting Help Online Advertising?*, 18TH INT'L CONF. ON THE WORLD WIDE WEB PROC. 261, 266 (2009).

of clicks that led to a sale) more than doubled (although these results were available only from five of the networks).[71]

Targeted advertising may be particularly useful for market segments that are new or unfamiliar to most consumers, where ads can inform consumers about the type of product or service as well as the particular offering within the category.[72] When customized advertising is sufficiently accurate, organizations may invest more in this form of communication than in untargeted advertising, even though the targeted ads reach a smaller cohort of consumers.[73] A 2012 study found that the key benefit of targeted advertising — increasing click-through rates ("CTR") from users who received the ad — was driven by selecting users who were interested in the advertising entity, rather than by the informational content of the ad itself.[74] Based upon data from the search engine Yahoo!, the study found that the marginal cost to induce someone to search for a particular brand was $15.65 for any user, but $1.69 for a targeted user.[75] By contrast, one recent study using data from a large media company found that the benefits of targeted ads versus untargeted ones are small: only about 4%.[76] That result differs greatly

[71] HOWARD BEALES, THE VALUE OF BEHAVIORAL TARGETING 3 (2010), https://www.ftc.gov/sites/default/files/documents/public_comments/privacy-roundtables-comment-project-no.p095416-544506-00117/544506-00117.pdf [https://perma.cc/63EB-QZGX].

[72] Shin & Yu, *supra* note 69, at 900. There is a trade-off: advertising educates consumers about the new category but also creates incentives for them to search for other competing producers within it. The payoff to firms depends on whether the prominence effect of being the first brand displayed to consumers is greater than the free-riding effect that its competitors gain from that organization's informational investment. *Id.* at 914.

[73] *Id.* at 914.

[74] Ayman Farahat & Michael Bailey, *How Effective is Targeted Advertising?*, 21ST INT'L CONF. ON WORLD WIDE WEB PROC. 111, 119 (2012), https://dl.acm.org/citation.cfm?id=2187852 [https://perma.cc/9PE5-TEME].

[75] *Id.*

[76] Veronica Marotta, Vibhanshu Abhishek & Alessandro Acquisti, Online Tracking and Publishers' Revenues: An Empirical Analysis 6 (May 2019) (unpublished manuscript), https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf [https://perma.cc/2WQV-5LVG].

from other studies and may reflect that publishers have varying degrees of reliance on targeted ads.[77]

C. Welfare Effects

Targeted advertising research has also examined the welfare effects of this type of marketing. Determining the impact of customized advertising on consumers is challenging both because people have inconsistent preferences regarding this technique[78] and because the effects of customization appear to be strongly context-specific.[79] Users have variegated[80] and often contradictory views of advertising,[81] including the targeted sort.[82] With targeted ads, they may dislike having information gathered about their activities and preferences — but they

[77] *See* Garrett A. Johnson, Scott K. Shriver & Shaoyin Du, *Consumer Privacy Choice in Online Advertising: Who Opts out and at What Cost to Industry?*, 39 MKTG. SCI. 33, 46-47 (2020).

[78] *See* Aleecia M. McDonald & Lorrie Faith Cranor, *Americans' Attitudes About Internet Behavioral Advertising Practices*, 9TH ANN. ACM WORKSHOP ON PRIVACY IN THE ELEC. SOC'Y PROC. 63, 70 (2010), https://doi.org/10.1145/1866919.1866929 [https://perma.cc/MX56-2Q3N] (finding 11% of respondents would pay $1 per month to avoid having their data collected for behavioral advertising, thereby gaining privacy, but 31% would accept $1 per month to disclose data for this purpose, suggesting consumer preferences are affected by initial allocation of privacy rights).

[79] *See* Louise Matsakis, *Online Ad Targeting Does Work — As Long as It's Not Creepy*, WIRED (May 11, 2018), https://www.wired.com/story/online-ad-targeting-does-work-as-long-as-its-not-creepy/ [https://perma.cc/F6V7-LYSE].

[80] *See* Sara Karlovitch, *Gen Z Is More Likely to Be OK with Targeted Ads — Here's What the Numbers Say*, MARKETING DIVE (Aug. 25, 2023), https://www.marketingdive.com/news/allow-tracking-younger-consumers-more-likely-okay-with-target/691452/ [https://perma.cc/9RDX-LNRB].

[81] *See* Anna Yukhananov, *Consumers Love to Hate Ads but Won't Pay to Escape Them*, MORNING CONSULT (Sept. 23, 2017), https://morningconsult.com/2017/09/23/consumers-love-hate-ads-wont-pay-escape/ [https://perma.cc/34N7-6SCZ] (reporting survey finding 75% of Americans view Internet advertising as intrusive, but 67% would not pay more for ad-free Internet content).

[82] Shelby Jordan, *Despite Negative Perceptions, 52% of Consumers Can Identify Benefits of Targeted Advertising*, PR NEWSWIRE (Mar. 25, 2021), https://www.prnewswire.com/news-releases/despite-negative-perceptions-52-of-consumers-can-identify-benefits-of-targeted-advertising-301255752.html [https://perma.cc/TD9Q-UZMX].

also hate irrelevant ads, especially ones that are of low-quality.[83] One 2018 survey found that 91% of consumers were more likely to shop with brands that offer personalized communications.[84] A 2020 study of consumer opt-out behavior demonstrated that users say one thing but do another: surveys consistently find that a large majority of Americans dislike targeted advertising online, but virtually none of them opt out of it when they have the opportunity to do so.[85] The advertising industry launched the AdChoices program in 2010 to enable consumers to opt out of behavioral advertising.[86] By 2012, AdChoices covered 90% of American behavioral advertising publishers.[87] Despite purportedly strong sentiment against targeted ads, consumers opted out of only 0.23% of ad impressions (displays), indicating that only 1 impression out of 441 resulted from an opt-out user.[88] The rate of behavioral advertising opt-outs in the United States is in line with rates in Canada and Europe, where AdChoices also operates: 0.16% in Canada, and 0.26% in Europe.[89] Americans claim to dislike behavioral advertising, but most take few measures to avoid it.[90]

Context matters for consumer perceptions of targeted ads. The higher prices for these ads may, ironically, serve an important gate-keeping function: as prices fall, especially in an environment of decreased spending on Internet advertising overall, lower-quality and less relevant advertisers can reach users.[91] Consumer preferences

[83] *See* Tiffany Hsu, *Why Are You Seeing So Many Bad Digital Ads Now?*, N.Y. TIMES (Feb. 11, 2023), https://www.nytimes.com/2023/02/11/technology/bad-digital-ads.html.

[84] *See* ACCENTURE INTERACTIVE, MAKING IT PERSONAL 3 (2018), https://www.accenture.com/content/dam/accenture/final/a-com-migration/pdf/pdf-83/accenture-making-personal.pdf [https://perma.cc/4P7L-4L9P].

[85] Johnson et al., *supra* note 77, at 39-40.

[86] *Id.* at 35-37.

[87] *Id.* at 36.

[88] *Id.* at 40.

[89] *Id.* The study collected data from June 15, which was before adoption of the European Union's General Data Protection Regulation, but after the adoption of the e-Privacy Directive in 2002 and its amendments in 2009. *See ePrivacy Directive*, EUR. DATA PROT. SUPERVISOR, https://edps.europa.eu/data-protection/our-work/subjects/eprivacy-directive_en (last visited Sept. 20, 2024) [https://perma.cc/777B-EPNB].

[90] *See* Johnson, Shriver & Du, *supra* note 77, at 36-37.

[91] *See* Hsu, *supra* note 83.

regarding targeted advertising are context-dependent in important ways. Commentators often employ the fitting but imprecise term "creepy" to describe advertising practices that diminish user acceptance of these ads.[92] For example, one study found that users viewed employing third-party data or generating inferences to be unsavory, but that recommendations based on past activity on the site were acceptable.[93] Thus, it is not only the information conveyed, but how and why it was communicated, that affects whether consumers find personalized ads acceptable.

There may also be important second-order welfare effects, such as on innovation, that arise from the regulatory treatment of targeted advertising. A 2023 study examined the effects on application development of Google's 2019 decision to ban targeted advertising in children's games that were distributed via its Google Play Store to users of the Android operating system.[94] The study compared games that were affected by the ban with those that were not and found that developers were 17% less likely to release feature updates and bug fixes for games where targeted advertising was prohibited.[95] Games that were more dependent on advertising showed larger decreases.[96] In addition, developers shifted resources from updates for children's games to ones for games where targeted advertising was still allowed.[97] The only exception was for highly popular games, which likely benefited from weakened competition or increased monetization potential.[98]

Finally, the effects of targeted advertising, both in absolute and relative terms, remain contested. One recent, influential study contends that the consumer welfare effects of targeted advertising are smaller than expected, and the causes are more complex than is typically

---

[92] *See* ACCENTURE INTERACTIVE, *supra* note 84, at 5.

[93] *See* Tami Kim, Kate Barasz & Leslie K. John, *Why Am I Seeing This Ad? The Effect of Ad Transparency on Ad Effectiveness*, 45 J. CONSUMER RSCH. 906, 920 (2019); Matsakis, *supra* note 79.

[94] Tobias Kircher & Jens Foerderer, *Ban Targeted Advertising? An Empirical Investigation of the Consequences for App Development*, 70 MGMT. SCI. 1070, 1071 (2024).

[95] *Id.* at 1079-80.

[96] *Id.* at 1080.

[97] *Id.* at 1088.

[98] *Id.*

understood.[99] In the study, targeted ads were more relevant than random ones, but were still not highly relevant to users.[100] Similarly, the products featured in targeted ads were of higher quality than those in random ads — but not as high-quality as ones available from searches for similar products to those in the targeted ads.[101] Welfare effects depended heavily on consumers' knowledge of the categories of products or services featured in the advertising and on the level of consumer effort required to determine the quality of the providers of those products or services.[102]

While debate persists about the overall social effects of targeted advertising, for advertisers, it is clearly the rational choice.

II. THE TECHNOLOGY

Internet advertising technology changes rapidly and on an uncertain timetable. This Part examines the latest disruptions, then briefly describes the technologies involved in gathering, analyzing, and displaying targeted ads.

A. Latest Developments

Three recent changes to advertising technology are particularly noteworthy: first, Apple's decision to limit access to device-specific identifiers unless a user opts in;[103] second, the increasing sophistication of algorithmic tools in the advertising ecosystem;[104] and third, the attempt by some popular platforms to move towards a "walled garden" architecture that constrains ads and other third-party content.[105] An even more momentous change looms: Google announced it will phase

[99] Mustri, Adjerid & Acquisti, *supra* note 47, at 3-4.

[100] *Id.* at 14.

[101] *Id.*

[102] *Id.*

[103] *See* Brian X. Chen, *To Be Tracked or Not? Apple Is Now Giving Us the Choice*, N.Y. TIMES, https://www.nytimes.com/2021/04/26/technology/personaltech/apple-app-tracking-transparency.html (last updated Sept. 29, 2021).

[104] *See* Hsu, *supra* note 83.

[105] *See* PWC, *supra* note 48, at 8 (stating that "[w]hile walled gardens have been present in advertising for some time, the recent focus on privacy in advertising has led to an increase in their utilization").

out third-party cookies beginning in the third quarter of 2024,[106] and it started testing this restriction on 1% of Chrome users on January 4, 2024.[107] Although commentators are skeptical that Google will meet its self-imposed deadline,[108] the end of third-party cookies — "cookie armageddon" — in the company's advertising architecture will be an epochal event whenever it occurs.[109]

In April 2021, Apple debuted its App Tracking Transparency ("ATT") feature with version 14.5 of its various operating systems.[110] ATT requires apps to get user permission before accessing the Apple device's system advertising identifier ("IDFA").[111] Users can decide on a per-app basis or set a default that blocks all access to the identifier.[112] Formally, Apple also forbade apps from tracking users via other personally identifiable information, such as an e-mail address, although that restriction was a matter of contractual authorization rather than a technological restriction.[113] ATT caused widespread consternation in the advertising industry; Meta, for example, predicted that it would lose $10 billion due to the change, although there is little data to substantiate that forecast.[114] Unsurprisingly, relatively few iPhone or Apple device

[106] *Third-Party Cookies*, GOOGLE PRIV. SANDBOX, https://developers.google.com/privacy-sandbox/3pcd (last visited Sept. 20, 2024) [https://perma.cc/FNR5-3Z36].

[107] *See* Joseph, *supra* note 29.

[108] *Id.*

[109] Seb Joseph, *'Dragging on for Too Long': Ad Execs Sound off on the Beginning of the End of Third-Party Cookies in Google's Chrome*, DIGIDAY (Jan. 8, 2024), https://digiday.com/marketing/dragging-on-for-too-long-ad-execs-sound-off-on-the-beginning-of-the-end-of-third-party-cookies-in-googles-chrome/ [https://perma.cc/G5ES-Q8WU] (quoting demand-side platform Preciso's CEO Piero Pavone).

[110] *See* Sara Morrison, *The Winners and Losers of Apple's Anti-Tracking Feature*, VOX (Apr. 29, 2022), https://www.vox.com/recode/23045136/apple-app-tracking-transparency-privacy-ads [https://perma.cc/GD2K-NQZM].

[111] *See* Chen, *supra* note 103.

[112] *See If an App Asks to Track Your Activity*, APPLE (Sept. 16, 2024), https://support.apple.com/en-us/HT212025 [https://perma.cc/J9PE-N8SA].

[113] *Id.* (noting Apple can remove offending apps from its App Store).

[114] *See* Kate Conger & Brian X. Chen, *A Change by Apple Is Tormenting Internet Companies, Especially Meta*, N.Y. TIMES (Feb. 3, 2022), https://www.nytimes.com/2022/02/03/technology/apple-privacy-changes-meta.html.

users opted in to tracking;[115] one survey put the number at only 24%.[116] Apple's decision to alter the default rules for targeted advertising on devices running its operating system were formally adopted to enhance user privacy,[117] but the change has also significantly enhanced the company's Search Ads business.[118] There is, however, little if any data suggesting that the adoption of ATT has had the predicted detrimental impact on advertisers.

Algorithms have established an increasingly important role in advertising online, but their prominence, and perhaps effectiveness, has exploded in the past several years.[119] This is one instance of a larger trend: the growing influence, and scrutiny, of what is popularly referred to as "artificial intelligence."[120] Automated software tools are involved in the vast majority of advertising purchases — over 90% in one estimate.[121] Artificial intelligence ("AI") is widely viewed as a promising,

[115] *See* RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE 8 (2009) (discussing power of default settings); Russell Korobkin, *Status Quo Bias and Contract Default Rules*, 83 CORNELL L. REV. 608, 612 (1998).

[116] Conger & Chen, *supra* note 114. Another analyst found that 27% of app installs in the first quarter of 2023 had an IDFA, meaning users opted in to sharing their identifiers with advertisers, compared with 70–80% IDFA availability before ATT implementation. Thomas Petit, *Small but Valuable: How to Leverage 27% of iOS Users with an IDFA*, APPSFLYER (Apr. 25, 2023), https://www.appsflyer.com/blog/measurement-analytics/leverage-users-using-idfa/ [https://perma.cc/ZYL3-EJMY].

[117] *See generally* APPLE, A DAY IN THE LIFE OF YOUR DATA (2021), https://www.apple.com/privacy/docs/A_Day_in_the_Life_of_Your_Data.pdf [https://perma.cc/APL9-XW2X].

[118] *See* Sarah Perez, *One Year Later, Apple's Privacy Changes Helped Boost Its Own Ads Business, Report Finds*, TECHCRUNCH (Sept. 6, 2022, 9:34 AM), https://techcrunch.com/2022/09/06/one-year-later-apples-privacy-changes-helped-boost-its-own-ads-business-report-finds/ [https://perma.cc/6U77-7WRK]; *Omdia Report Finds Apple's Ads Business Now Worth $3.7bn Per Year Following IDFA Changes*, OMDIA (Feb. 16, 2022), https://omdia.tech.informa.com/pr/2022/feb/omdia-report-finds-apples-ads-business-now-worth-3-7bn-per-year-following-idfa-changes (finding 264% advertising revenue growth in 2021 versus 2020).

[119] *See generally* Hairong Li, *Special Section Introduction: Artificial Intelligence and Advertising*, 48 J. ADVERT. 333 (2019).

[120] Artificial intelligence has formally been a field in computer science since 1956. *See Artificial Intelligence Coined at Dartmouth*, DARTMOUTH, https://home.dartmouth.edu/about/artificial-intelligence-ai-coined-dartmouth (last visited Sept. 17, 2024) [https://perma.cc/2MXJ-7N5R].

[121] *See* Hsu, *supra* note 83.

threatening, and highly disruptive technology for advertising. Google declared "code red" based on the perceived threat of machine learning techniques to its advertising business, and some (likely overheated) estimates suggest that AI will disrupt $500 billion in digital advertising.[122] Generative AI, such as ChatGPT and DALL-E, is seen as the leading edge of the disruption. Although perceptions of the capabilities of AI are widely overstated,[123] the increasing sophistication of algorithmic processing of Big Data is unquestionably affecting online advertising.[124]

Finally, some major platforms have begun to limit third-party access to their content or users, largely as a defensive measure to protect revenues. Apple's ATT is a leading example. Facebook's algorithm seems to deprecate posts with links to external content, likely because such posts draw users away from the social media site, thereby decreasing their engagement score and value to Facebook.[125] Twitter has all but eliminated free access to its content via its Application Programming Interface ("API") for academic researchers, with the goals of pushing developers to upgrade to more lucrative paid options and blocking third-party clients from displaying its content.[126] Although some of these changes may be reactions to the recent slowdown in advertising spending online, some predate that shift, reflecting a separate change in strategy.[127]

---

[122] *See* Tripp Mickle, Cade Metz & Nico Grant, *The Chatbots Are Here, and the Internet Industry Is in a Tizzy*, N.Y. TIMES (Mar. 8, 2023), https://www.nytimes.com/2023/03/08/technology/chatbots-disrupt-internet-industry.html.

[123] *See* Derek E. Bambauer & Mihai Surdeanu, *Authorbots*, 3 J. FREE SPEECH L. 375, 379 (2023); Timothy B. Lee, *Software Didn't Eat the World*, SLATE (Apr. 24, 2023, 9:00 AM), https://slate.com/technology/2023/04/artificial-intelligence-jobs-software-eating-the-world-andreessen-economy.html [https://perma.cc/2HKQ-JPV2].

[124] *See* Vanian, *supra* note 42.

[125] *See* Elena Cucu, [*What Data Says*] *Where to Place Links in Facebook Posts for Greater Engagement. Here's What 51,054,216 Facebook Posts Tell Us*, SOC. INSIDER (Oct. 26, 2021), http://thesocialinsider.org/index-83.html [https://perma.cc/C52X-8R3A].

[126] *See* Ivan Mehta, *New Twitter API Tiers Still Miss the Mark, Developers Say*, TECHCRUNCH (Mar. 30, 2023, 8:39 AM), https://techcrunch.com/2023/03/30/new-twitter-api-tiers-still-miss-the-mark-developers-say/ [https://perma.cc/Y92S-FLX5].

[127] *See Are Walled Gardens in 2024 Still a Marketing Challenge?*, EXPERIAN (Nov. 16, 2023), https://www.experian.com/blogs/marketing-forward/walled-gardens-in-2024/ [https://perma.cc/VD6R-SWSJ].

B. Gathering Data

Targeted advertising collects three types of user data: that which consumers voluntarily share; that which is inherently shared by their software or network; and that which the app or Web site actively gathers. Users can employ their own technological measures to prevent data collection, although doing so requires some skill.

Information that is voluntarily disclosed depends relatively little upon the underlying technology, although the design of applications or Web sites can make sharing data easier, such as by providing a dropdown list of responses rather than a blank text box for free-form entry.[128] An app may ask users to provide information such as an e-mail address, ZIP code, and age in exchange for accessing the application's features.[129] Gathering this data is principally a function of users' willingness to disclose personal information rather than any particular technological capability.

By contrast, information that is inherently shared can vary dramatically with the technology at issue, including the user's operating system (such as Microsoft Windows or Apple iOS), application, communications protocol, and security software. However, advertisers can typically rely on a baseline of consumer information that is typically disclosed regardless of design.[130] The collection of this information is commonly called "fingerprinting," and it is becoming more common as other technical mechanisms for targeting, such as cookies, become more

[128] Ironically, guiding users towards disclosure in this way can increase the risk of liability for the creator or operator of the app or site. *See* Fair Hous. Council v. Roommates.com, 521 F.3d 1157, 1164-72 (9th Cir. 2008) (finding that Roommates.com was not eligible for immunity provided by Section 230, 47 U.S.C. § 230, because its "website is designed to force subscribers to divulge protected characteristics and discriminatory preferences" in possible violation of the federal Fair Housing Act).

[129] *See* Kenneth A. Bamberger, Serge Egelman, Catherine Han, Amit Elazari Bar On & Irwin Reyes, *Can You Pay for Privacy? Consumer Expectations and the Behavior of Free and Paid Apps*, 35 BERKELEY TECH. L.J. 327, 330, 350 (2020).

[130] The Webkay site provides a useful demonstration. *See What Every Browser Knows About You*, WEBKAY, https://webkay.robinlinus.com/ (last visited Sept. 19, 2024) [https://perma.cc/JVB7-M7LP]. Cover Your Tracks provides similar data. *See, e.g.*, *Cover Your Tracks*, ELEC. FRONTIER FOUND., https://coveryourtracks.eff.org/ (last visited Sept. 17, 2024) [https://perma.cc/8J85-99XY].

heavily regulated[131] or blocked.[132] Fingerprinting can generally obtain details about a user's IP address, operating system, device hardware,[133] physical location, connection speed, system settings, and even content previously accessed.[134] This information is available because revealing it is often the price for using interactive Internet technologies, especially on mobile devices.

Active efforts by the Web site or app can collect an extensive range of data. The information may be collected by the site or app itself; by a third-party entity with code running on that site or app;[135] or both. Common techniques include the now-ubiquitous cookie file,[136] Web

[131] *See* Matt Burgess, *The Quiet Way Advertisers Are Tracking Your Browsing*, WIRED (Feb. 26, 2022, 7:00 AM), https://www.wired.com/story/browser-fingerprinting-tracking-explained/.

[132] *See supra* notes 106–109.

[133] *Bill Toulas*, *Researchers Use GPU Fingerprinting to Track Users Online*, BLEEPING COMPUT. (Jan. 30, 2022, 10:12 AM), https://www.bleepingcomputer.com/news/security/researchers-use-gpu-fingerprinting-to-track-users-online/ [https://perma.cc/H3D8-WF8X].

[134] *See* Susan Landau & Patricia Vargas Leon, *Reversing Privacy Risks: Strict Limitations on the Use of Communications Metadata and Telemetry Information*, 21 COLO. TECH. L.J. 225, 238-41, 270-96 (2023).

[135] The site or app may not be aware of the third-party code. *See* Christopher Boyd, *The Danger of Third Parties: Ads, Pipelines, and Plugins*, MALWAREBYTES LABS (July 20, 2018), https://www.malwarebytes.com/blog/news/2018/07/third-party-dangers-ads-pipelines-and-plugins [https://perma.cc/7SYF-6SE5].

[136] A different technique is the so-called "supercookie," which mimics the behavior of a traditional cookie through an unrelated mechanism. Supercookies are a genus of techniques, though, rather than any particular method. Embedding a unique identifier in a shared image resource that is cached by a browser is one, but only one, supercookie technique. *See,* Shubham Agarwal, *Browsers Are Rushing to Stop Shadowy "Supercookies" that Spy on Your Activity*, FAST CO. (Feb. 10, 2021), https://www.fastcompany.com/90602566/browser-supercookies-chrome-firefox-safari.

bugs,[137] activity tracking,[138] fingerprinting using HTML5,[139] WebGL,[140] the Web Audio API or AudioContext,[141] and shared resources.[142]

Users are not helpless against data collection technology. Consumers can control some data that is collected about them, even inherent data such as browser version, by employing different or additional software programs.[143] For example, the Tor browser and network attempt to prevent fingerprinting through measures such as routing traffic through an encrypted network.[144] The Brave browser adds random noise to inherent data.[145] These defenses are essentially mirror images: Tor tries to make users look alike even when they are different, and Brave tries to make similar users appear dissimilar. Vendors such as Apple and Mozilla have introduced changes to their software to reduce the data that users

[137] *Web Bug*, NAT'L INST. OF STANDARDS & TECH., https://csrc.nist.gov/glossary/term/web_bug (last visited Sept. 17, 2024) [https://perma.cc/8UVZ-LW5E].

[138] *See Tracking User Activity in Web Applications: Effective Tactics & Tools*, USERPILOT (Jan. 22, 2024), https://userpilot.com/blog/tracking-user-activity-in-web-applications/ [https://perma.cc/XU2V-3H8M].

[139] *See* KEATON MOWERY & HOVAV SHACHAM, PIXEL PERFECT: FINGERPRINTING CANVAS IN HTML5 1, https://hovav.net/ucsd/dist/canvas.pdf (last visited Sept. 17, 2024) [https://perma.cc/N6SY-8QNU].

[140] *See* Shujiang Wu, Song Li, Yinzhi Cao & Ningfei Wang, *Rendered Private: Making GLSL Execution Uniform to Prevent WebGL-based Browser Fingerprinting*, 28TH USENIX SEC. SYMP. 1 (2019), https://www.usenix.org/system/files/sec19-wu-shujiang.pdf [https://perma.cc/D2AM-5EDV].

[141] *See* Steven Englehardt & Arvind Narayanan, *Online Tracking: A 1-Million-Site Measurement and Analysis*, https://www.cs.princeton.edu/~arvindn/publications/OpenWPM_1_million_site_tracking_measurement.pdf (last visited Sept. 17, 2024) [https://perma.cc/GYC3-64CN].

[142] *See* Shubham Agarwal, *Your Digital Fingerprint Is Tracked Everywhere Online. Brave Wants to Change That*, DIGIT. TRENDS (June 10, 2021), https://www.digitaltrends.com/computing/digital-fingerprinting-online-privacy-brave/ [https://perma.cc/82G3-FB6V].

[143] *See* Stephen B. Wicker & Kolbeinn Karlsson, *Internet Advertising: Technology, Ethics, and a Serious Difference of Opinion*, 60 COMMC'NS ACM 70, 74-75 (2017).

[144] *See* Michael Muchmore, *Tor Browser Review*, PCMAG (Aug. 31, 2023), https://www.pcmag.com/reviews/tor-browser [https://perma.cc/46D7-MEY5].

[145] Brave Privacy Team, *Fingerprinting Defenses 2.0*, BRAVE (May 18, 2020), https://brave.com/privacy-updates/4-fingerprinting-defenses-2.0/ [https://perma.cc/4HSY-CSWX].

reveal involuntarily.[146] However, data gathering methods and mechanisms for blocking those methods co-evolve in a technological arms race, and methods intended to reduce data exposure may instead increase it. For example, browsers allow users to select a Do Not Track ("DNT") setting, indicating that they do not wish sites or apps to gather data about them. Sites and apps do not need to respect this preference, though, and indeed may employ a user's DNT setting as one additional piece of data.[147]

In short, the online environment is awash in data about users. The next Section describes how firms analyze this data.

C. Analyzing Data

Automated methods that employ sophisticated algorithms, such as machine learning, enable firms to discern consumer characteristics and preferences for advertising purposes with ever-increasing depth and precision. Algorithms have tremendous potential to analyze enormous volumes of data rapidly and efficiently. However, they also raise concerns about fairness, accountability, and transparency.[148] Unfortunately, efforts to make algorithms more explainable may not be possible given how these mathematical models function.[149]

---

[146] *See Apple Advances Its Privacy Leadership with iOS 15, iPadOS 15, macOS Monterey, and watchOS 8*, APPLE (June 7, 2021), https://www.apple.com/newsroom/2021/06/apple-advances-its-privacy-leadership-with-ios-15-ipados-15-macos-monterey-and-watchos-8/ [https://perma.cc/K5CA-Q5W9]; Christopher Boyd, *Firefox Stops Advertisers Tracking You as You Browse, Calls Itself the Most "Private and Secure Major Browser,"* MALWAREBYTES LABS (June 15, 2022), https://www.malwarebytes.com/blog/news/2022/06/firefox-stops-advertisers-tracking-you-as-you-browse-calls-itself-the-most-private-and-secure-major-browser [https://perma.cc/84PU-N84U]. *But see* Christopher Boyd, *Google Delays Chrome Third Party Cookie Sunsetting . . . Again*, MALWAREBYTES LABS (July 29, 2022), https://www.malwarebytes.com/blog/news/2022/07/google-delays-chrome-third-party-cookie-sunsetting-again [https://perma.cc/XM4F-ECJH].

[147] *See* Kashmir Hill, *"Do Not Track," the Privacy Tool Used by Millions of People, Doesn't Do Anything*, GIZMODO (Oct. 15, 2018), https://gizmodo.com/do-not-track-the-privacy-tool-used-by-millions-of-peop-1828868324 [https://perma.cc/M2PP-X383].

[148] *See* Sonia K. Katyal, *Private Accountability in the Age of Artificial Intelligence*, 66 UCLA L. REV. 54, 111-17 (2019).

[149] *See* Chloe Xiang, *Scientists Increasingly Can't Explain How AI Works*, VICE (Nov. 1, 2022, 9:00 AM), https://www.vice.com/en/article/y3pezm/scientists-increasingly-cant-explain-how-ai-works [https://perma.cc/C9UW-AFTD].

Targeting based on inferred consumer characteristics is a well-established practice. Advertisers have long used rough proxies to reach audiences they believe will be receptive to their pitches. For example, with broadcast television, the long-running Nielsen ratings provided some insight into the characteristics of at least a sample of viewers.[150] The ratings were a critical factor in both pricing and placement of ads — although both the PGA (golf) and the NBA (basketball) are popular televised sports events, their audiences differ dramatically in demographics, as reflected in the Nielsen data, and the ads shown during each telecast reflect that.[151] Similar crude techniques characterized early e-commerce. The online travel site Orbitz gained unwanted notoriety when it displayed higher-priced options to users with Apple computers than to users running Microsoft Windows.[152]

Current algorithmic models that analyze consumer data to select ads are far more sophisticated. Facebook, for example, uses machine learning models in combination with its own datasets and third party datasets to achieve highly customizable targeting of ads via methods that remain relatively opaque.[153] Advertisers who want to display content on Facebook can choose from a list of characteristics to

[150] *See* James Miller & James E. Prieger, *The Broadcasters' Transition Date Roulette: Strategic Aspects of the DTV Transition*, 9 J. ON TELECOMM. & HIGH TECH. L. 437, 453-55 (2011).

[151] *See* NIELSEN, FANS ARE CHANGING THE GAME: 2022 GLOBAL SPORTS MARKETING REPORT 6-8 (2022); Ricky Clemons, *PGA Tour, LIV Golf Fight for Diverse, Millennial Fans and the Future of Golf*, BAY STATE BANNER (Aug. 31, 2022), https://www.baystatebanner.com/2022/08/31/pga-tour-liv-golf-fight-for-diverse-millennial-fans-and-the-future-of-golf/ [https://perma.cc/5KCD-P7VU].

[152] *See* Anita Ramasastry, *The Orbitz Controversy: Why Steering Mac Users Toward Higher-Priced Hotels Is Arguably Wrong, and What Might be Done About It*, VERDICT (July 3, 2012), https://verdict.justia.com/2012/07/03/the-orbitz-controversy-why-steering-mac-users-toward-higher-priced-hotels-is-arguably-wrong-and-what-might-be-done-about-it [https://perma.cc/7KZ6-4GSP].

[153] Athanasios Andreou, Márcio Silva, Fabrício Benevenuto, Oana Goga, Patrick Loiseau & Alan Mislove, *Measuring the Facebook Advertising Ecosystem*, NETWORK & DISTRIBUTED SYS. SEC. SYMP. (2019), https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_04B-1_Andreou_paper.pdf [https://perma.cc/4MGB-3SPD].

determine which users should see their ads.[154] In addition, Facebook offers the option to display ads to users that its proprietary algorithm deems similar to the ones that an advertiser has selected.[155] Thus, Facebook is using analytical techniques to make inferences: its software uses data that does not directly disclose the consumer preference at issue but enables prediction of the preference with a specified degree of accuracy.[156] Combining datasets offers Facebook, and other platforms and advertisers, greater ability to detect preferences and, if necessary, to infer them.

Ironically, a significant challenge for advertisers is aggregating data to determine the success of their content. Data about a given ad's success, such as the frequency with which users interact with the ad when it is displayed to them, are often separated into different data stores across companies or, as in the case of Facebook, within the same firm.[157] Researchers have developed techniques using algorithms to retrieve and analyze this data, but results are still often incomplete.[158]

Analyzing data about consumer preferences is at the heart of targeted advertising and, at a broader scale, at the core of the business model for many if not most online firms.[159] The next Section explores how advertisers display content to users.

---

[154] *Id.* In 2021, Facebook limited the level of ad targeting advertisers can employ on sensitive issues such as politics, race, and sexual orientation. *See* Jeff Horwitz, *Facebook Parent Meta Limits Ad Targeting for Politics and Other Sensitive Issues; CEO Mark Zuckerberg had Overruled Staffers Last Year When They Pushed for Similar Changes*, WALL ST. J. (Nov. 9, 2021, 4:34 PM), https://www.wsj.com/articles/facebook-parent-meta-bans-targeting-for-political-ads-11636488053.

[155] *Id.*; Andreou, Silva, Benevenuto, Goga, Loiseau & Mislove, *supra* note 153.

[156] *See* Muhammad Ali, Piotr Sapiezynski, Aleksandra Korolova, Alan Mislove & Aaron Rieke, *Ad Delivery Algorithms: The Hidden Arbiters of Political Messaging*, (Dec. 17, 2019), https://arxiv.org/pdf/1912.04255.pdf [https://perma.cc/44B4-VLJZ].

[157] *See* Sam Biddle, *Facebook Engineers: We Have No Idea Where We Keep All Your Personal Data*, INTERCEPT (Sept. 7, 2022, 7:00 AM), https://theintercept.com/2022/09/07/facebook-personal-data-no-accountability/ [https://perma.cc/9AYQ-NKL2].

[158] *See* Joni Salminen, Tommi Salenius & Bernard J. Jansen, *SiloSolver: Developing an Algorithm for Automatic Aggregation and Testing of Isolated Customer Segments in Facebook Ads Campaigns*, 2ND INT'L CONF. ON INTELLIGENT DATA SCI. TECHS. & APPLICATIONS 6-9 (2021).

[159] *See, e.g.*, Dan Balz, *How the Obama Campaign Won the Race for Voter Data*, WASH. POST (July 28, 2013, 8:09 PM), https://www.washingtonpost.com/politics/how-the-

D. Delivering Content

Advertising content (known in the industry as the "ad creative") may be produced and distributed by the platform or application upon which it appears, or there may be a third-party source involved, such as an advertising network. With third-party ad creatives, a platform operates in a two-sided market: it offers services to both users and advertisers.[160] Some services, such as Amazon Prime, use both forms: content produced by Amazon, such as the series "The Expanse," generally only features ads for other Amazon content, while third-party material, such as series from non-Amazon studios, can include ads for other things.[161] Platforms and advertisers may each hold information about users, which they may share.

The mechanisms by which a site that accepts third-party ad content decides upon which ad to display are becoming more sophisticated. Ad auctions are common,[162] enabling advertisers to compete to bid on ads targeted to a particular set of user characteristics, sometimes including personally identifiable information.[163] As advertising becomes more targeted and sophisticated, its pricing does the same, creating incentives for advertisers to refine both their targeting and pricing mechanisms.[164]

Finally, content delivery depends critically upon the technological state of a user's device. Consumers have a wide range of devices with software that is up to date — or not — in highly variable ways.[165] The

obama-campaign-won-the-race-for-voter-data/2013/07/28/ad32c7b4-ee4e-11e2-a1f9-ea873b7e0424story.html.

[160] *See* David S. Evans, *The Economics of the Online Advertising Industry*, 7 REV. NETWORK ECON. 359, 378-79 (2008).

[161] *See* Ruben Circelli, *I Pay for Amazon Prime Video, So Why Am I Seeing Ads?*, WHAT HI-FI? (May 18, 2022), https://www.whathifi.com/features/i-pay-for-amazon-prime-video-so-why-am-i-seeing-ads [https://perma.cc/2GFV-ZETZ].

[162] *See* Joshua A.T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 DUKE L.J. 385, 429-30 (2015).

[163] These mechanisms are constantly updated. For a readable account of how Facebook's Ad Algorithm worked in 2018. *See* Michael Stelzner, *The Facebook Ad Algorithm: What Marketers Need to Know*, SOC. MEDIA EXAM'R (Aug. 17, 2018), https://www.socialmediaexaminer.com/facebook-ad-algorithm-ralph-burns/.

[164] *See* Fairfield & Engel, *supra* note 162, at 430.

[165] *See* Colleen McClain, Michelle Faverio, Monica Anderson & Eugenie Park, *How Americans Protect Their Online Data*, PEW RSCH. CTR. (Oct. 18, 2023),

more significant challenge, though, is self-help by consumers who do not want to see certain ads or any ads at all. Roughly 40% of American Internet users use ad-blocking software.[166] Their reasons for doing so include worries about intrusive content, security, bandwidth usage, and privacy.[167] The Chrome browser on Google's Android operating system includes ad-blocking capability that, by default, blocks content that it perceives to violate the Better Ad Standards.[168] Ad blocking has both technological and financial consequences. Technologically, it leads to an arms race: advertisers who develop new or different mechanisms for delivering content may be able to avoid blocking software, increasing the rate at which targeted users see their material.[169] Financially, advertisers can predict that their content will not reach a sizable fraction of users to whom it is delivered, and they will reduce the prices they pay (or can charge) accordingly.[170] Of course, a user's behavior with ad blocking software could itself become part of their preference profile;

https://www.pewresearch.org/internet/2023/10/18/how-americans-protect-their-online-data/#how-people-are-protecting-their-digital-privacy [https://perma.cc/S8G6-WJL8] (finding 17% of adult American smartphone users update the operating system only when required to, along with 21% for applications).

[166] The number varies with the source but seems to hover between 31% and 40%. *See* Backlinko Team, *Ad Blocker Usage and Demographic Statistics*, BACKLINKO, https://backlinko.com/ad-blockers-users (last updated Sept. 2, 2024) [https://perma.cc/P2AB-B6J2]; James Wohr, *Ad Blocking: What It Is and Why It Matters to Marketers and Advertisers,* EMARKETER (Sept. 4, 2024), https://www.insiderintelligence.com/insights/ad-blocking/ [https://perma.cc/T6LQ-KFQC] (quoting 31% figure from March 2023).

[167] *See Ad Blockers – What Are They – How They Impact Digital Ad Effectiveness*, MARTECH SERIES (Dec. 7, 2023), https://martechseries.com/mts-insights/staff-writers/ad-blockers-what-they-are-how-they-impact-digital-ad-effectiveness/ [https://perma.cc/6JTL-LY9X].

[168] *Visit a Site by Turning off Chrome's Ad Blocker*, GOOGLE, https://support.google.com/chrome/answer/7632919?hl=en&co=GENIE.Platform%3DAndroid (last visited Sept. 17, 2024) [https://perma.cc/C244-HK4Y].

[169] *See* Anthony Ha, *Inside the "Arms Race" Between Youtube and Ad Blockers*, ENGADGET (Dec. 1, 2023), https://www.engadget.com/inside-the-arms-race-between-youtube-and-ad-blockers-140031824.html [https://perma.cc/PR9T-DVL5].

[170] *See id.*

consumers who employ ad blockers have different purchasing patterns than ones who do not.[171]

The technological makeup of the advertising ecosystem creates a set of capabilities and constraints with which advertisers, users, platforms, and regulators must contend, even as that landscape changes constantly.

III. THE RISKS

While targeted advertising raises a number of concerns, privacy harms are at the core of the most strongly felt and fervently advanced objections to the practice. This Part locates the most pressing privacy concerns within a taxonomy based on the advertising life cycle, helping to identify the keys to mitigate these risks.

Defining "privacy" is a challenge.[172] The term gained prominence in American legal theory in 1890 when Samuel Warren and Louis Brandeis described the concept as the "right to be let alone."[173] Subsequently, privacy's meaning has shifted,[174] blurred, and become deeply contested.[175] Privacy means something different altogether in Europe, even though Warren and Brandeis plainly intended "to introduce a

[171] *See* Vilma Todri, *Frontiers: The Impact of Ad-blockers on Online Consumer Behavior*, 41 MKTG. SCI. 7, 7 (2022), https://doi.org/10.1287/mksc.2021.1309 [https://perma.cc/6D44-ND5S].

[172] *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 479-84 (2006).

[173] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

[174] *See, e.g.*, Abraham Bell & Gideon Parchomovsky, *The Privacy Interest in Property*, 167 U. PA. L. REV. 869, 872 (2019) (noting that "the roots of modern constitutional privacy law are to be found in concepts of property . . . privacy interests were originally thought to be defined by, and in service of, property rights"). *But see* Jane R. Bambauer, *How to Get the Property Out of Privacy Law*, YALE L.J.F. 1087, 1091 (2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4629539 [https://perma.cc/AVA3-CD5L].

[175] *See* ANITA L. ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? 25 (2011); Alessandro Acquisti, Curtis Taylor & Liad Wagman, *The Economics of Privacy*, 54 J. ECON. LIT. 442, 442 (2016); Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1852 (2010); Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1905 (2013); Jerry Kang, *Information Privacy in Cyberspace Transactions,* 50 STAN. L. REV. 1193, 1200 (1998); Solove, *supra* note 172, at 478.

continental-style right of privacy into American law."[176] Even if one adopted a coherent conception of privacy, privacy law is indeterminate: constantly balanced against competing values, full of exceptions, and technologically dependent.[177]

This Article adopts a pragmatic working definition — privacy is the "normative framework for deciding who should legitimately have the capability to access and alter information."[178] This characterization usefully encompasses privacy in the form of law (backed by the threat of compulsion by the state), in the form of norms (enforced through reputational sanctions and social disapprobation), and other modalities.[179] It recognizes that privacy is frequently not a rigorously defined intellectual creation, but instead an emotional reaction driven by a perceived violation of a felt but somewhat inchoate belief.[180] Put bluntly, some behavior simply seems creepy, even if what counts as creepy varies greatly based upon the observer.[181] That quality can make privacy objections harder to address, but it also provides them with force. Privacy is contested territory. This Part's goal is descriptive: to survey the landscape of privacy issues in targeted advertising without opining on their worth or coherence. It does so through the lens of an advertisement's life cycle.

A. Life Cycle

This Section uses the concept of the life cycle of an advertisement as an organizing principle for privacy concerns. This approach helps map privacy issues to relevant entities within the advertising ecosystem.

---

[176] James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1204 (2004).

[177] *See* Ryan Calo, *Privacy Law's Indeterminacy*, 20 THEORETICAL INQUIRIES L. 33, 34 (2019).

[178] Derek E. Bambauer, *Privacy Versus Security*, 103 J. CRIM. L. & CRIMINOLOGY 667, 669 (2013) [hereinafter Bambauer, *Privacy Versus Security*].

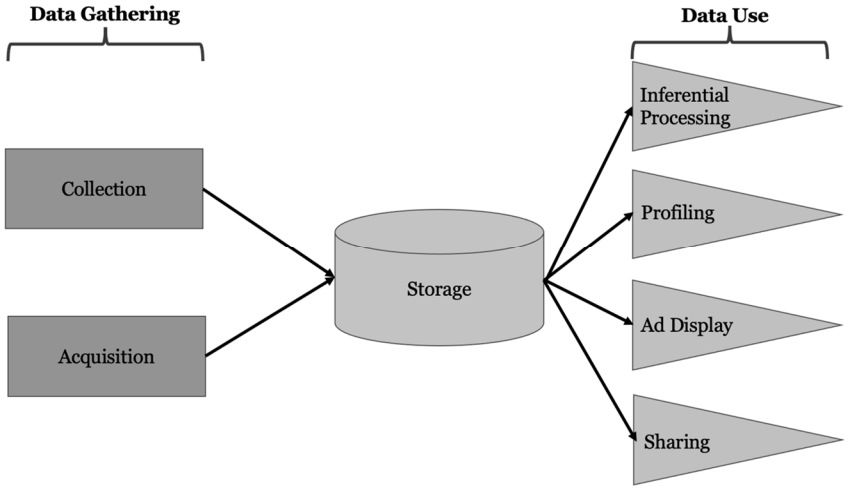
[179] *See, e.g.*, Richard H. McAdams, *Group Norms, Gossip, and Blackmail*, 144 U. PA. L. REV. 2237, 2239-40 (1996).

[180] *See* Whitman, *supra* note 176, at 1154-55.

[181] *See* Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 16 YALE J.L. & TECH. 59, 60 (2013).

Figure 1 depicts the information flow in the advertising life cycle, beginning at the left and moving right over time.

FIGURE 1. ADVERTISING LIFE CYCLE



Targeted advertising requires gathering information to function. There are two basic ways for advertisers to come by data: collect the information themselves, such as tracking activities on a Web site or app; or acquire it from an entity already in possession. These two methods of obtaining the ingredients for targeting one's advertising are depicted at the left side of Figure 1; a given firm or advertiser may utilize one or both.

Next, the firm or advertiser will need to store that information, even if only briefly, to make use of it. The step of storing information that will, or could, be used for targeted advertising may create privacy worries unrelated to advertising itself; indeed, the datastore may be an attractive target for attackers.[182] Storage of information for advertising purposes is depicted in the center of Figure 1.

Finally, firms use information in ways that generate privacy concerns.[183] There are at least four broad categories of such uses. First, advertising data can be used, alone or in combination with other

[182] *See* Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 251 (2007).

[183] *See* Mark Verstraete, *Inseparable Uses*, 99 N.C. L. REV. 427, 429 (2021).

information, to generate new insights about consumers. Data processing that leads to new inferences may, however, reveal information about consumers that they do not wish to share or may not even know themselves.[184]

The second use is profiling: firms may process data to categorize consumers — for example, as members of a particular political group, or as fans of a genre of movies. There are several potential problems with profiling. The category into which individuals are placed may be insufficiently nuanced: members of the Green Party, for example, have similar political views but are hardly homogeneous in other preferences.[185] This can have minor repercussions, such as receiving irrelevant advertising, or major ones, such as being associated with the category beyond the advertising context.[186] These concerns worsen if the classification is erroneous.

The third and perhaps most obvious use of data is to select which advertising content to display to a user. The use of data to match ad content to consumer is likely the dominant use of consumer information in targeted advertising.

The final use of gathered data is to transact in the data itself. Thus, an advertiser might share its data store with a subsidiary or license access to it to another entity. This complements the earlier point that the entity holding the data may not have gathered it directly, but rather obtained it from a third party.

---

[184] One of the most widely cited stories involves Target predicting that a customer was pregnant even before her family knew. *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG. (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

[185] *See* James McBride, *How Green-Party Success Is Reshaping Global Politics*, COUNCIL ON FOR. RELS, https://www.cfr.org/backgrounder/how-green-party-success-reshaping-global-politics (last updated May 5, 2022) [https://perma.cc/DVG5-GF57].

[186] To sharpen the example, imagine the consumer is classified as belonging to the National Socialist (Nazi) party instead of the Greens. The advertising that this consumer might receive could be highly offensive, and the real-world consequences of being viewed as a Nazi might be severe. *See, e.g.*, Ayana Archie, *Elon Musk Is Being Sued for Libel for Accusing a Man of Having Neo-Nazi Links*, NPR (Oct. 4, 2023), https://www.npr.org/2023/10/04/1203339945/elon-musk-neo-nazi-defamation-lawsuit-ben-brody [https://perma.cc/K9DS-CTMW] (describing how false accusation of being a neo-Nazi led to online attacks).

B. Privacy Concerns by Life Cycle Stage

This Section assesses the major extant privacy concerns at each stage of the advertising life cycle, with two caveats. First, there are more concerns than this brief treatment can address; the effort here is to highlight privacy issues that have been particularly pervasive or appear especially worrisome. Second, this description is a snapshot: privacy concerns change constantly.

Many of these harms are multi-valenced: they are subject to multiple classifications and could be regulated under multiple regimes. Focusing on the privacy-related aspects of these harms is not intended to deprecate other concerns. Rather, it recognizes that injuries are often accretive, and thus privacy problems compound the harm. Fortunately, remedies for privacy harms may have spillover benefits in other areas.

Privacy harms may be particularly challenging because they are deontological: consumers can experience injuries that do not result in physical harm or financial disadvantage.[187] One might experience fear or revulsion, for example, based upon the knowledge that a data broker possesses certain personal information, even if no tangible adverse consequences occur.[188] Recognizing such injury is fully in keeping with American legal traditions, which have long protected against deontological harms. Tort law, for example, recognizes liability for placing a person in a false light.[189] Unlike defamation, false light (one of the four classic privacy torts identified by William Prosser)[190] compensates not for pecuniary damage to reputation but for emotional injury.[191] And the First Amendment confers protection against government regulations even if the speaker has nothing to gain from expressing themselves — autonomy interests are at the core of free

[187] *See* Anita Bernstein, *Real Remedies for Virtual Injuries*, 90 N.C. L. REV. 1457, 1457 (2012); Daniel Susser & Vincent Grimaldi, *Measuring Automated Influence: Between Empirical Evidence and Ethical Values*, PROC. 2021 AAAI/ACM CONF. ON AI, ETHICS, & SOC'Y 242, 248 (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3848919 [https://perma.cc/X2L6-ES4Z].

[188] *See* Anuj Puri, *A Theory of Group Privacy*, 30 CORNELL J.L. & PUB. POL'Y 477, 520 (2021).

[189] *See* RESTATEMENT (SECOND) OF TORTS § 652E (AM. L. INST. 1997).

[190] William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).

[191] *See, e.g.*, Godbehere v. Phoenix Newspapers, Inc., 162 Ariz. 335 (1989).

speech doctrine.[192] Assessing deontological harms can lead to important policy proposals — for example, Anita Allen has argued that autonomy concerns generate a normative obligation to respect not only the privacy of others, but one's own privacy.[193] Finally, deontological concerns may mean that consumer opposition to targeted advertising by itself counts as harm in the policy calculus.[194]

Like privacy itself, some privacy harms are dynamic and context dependent. Consumer preferences are malleable, leading to concerns about manipulation.[195] It may be possible to charge more, for example, if one advertises a sandwich to a consumer who is hungry, or if one offers quick shipment of ink to an author whose printer has just run dry. Cognitive biases may create vulnerabilities that targeted advertising could exploit.[196]

Finally, privacy harms from targeted advertising may be unevenly distributed. For example, majoritarian groups might see benefits from receiving better terms and offers, while marginalized communities might suffer particular harm from being excluded.[197] Thus, privacy harms from advertising may worsen existing social woes such as racial discrimination.[198] This imbalance may also skew the political economy

---

[192] *See* Richard H. Fallon, Jr., *Two Senses of Autonomy*, 46 STAN. L. REV. 875, 875 (1994).

[193] *See* Anita L. Allen, *Protecting One's Own Privacy in a Big Data Economy*, 130 HARV. L. REV. F. 71, 75 (2016); Anita L. Allen, *An Ethical Duty to Protect One's Own Information Privacy?*, 64 ALA. L. REV. 845, 864 (2013).

[194] *See* Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley & Michael Hennessy, *Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities That Enable It* 4 (2009), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214 [https://perma.cc/DZJ8-CUVC].

[195] *See* Jamie Liguri & Lior Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. LEGAL ANALYSIS 43, 44 (2021); Daniel Susser, Beate Rossler & Helen Nissenbaum, *Technology, Autonomy, and Manipulation*, 8 INTERNET POL'Y REV. 1, 1 (2019).

[196] *See generally* Derek E. Bambauer, *Shopping Badly: Cognitive Biases, Communications, and the Fallacy of the Marketplace of Ideas*, 77 U. COLO. L. REV. 649, 692-94 (2006); Amos Tversky & Daniel Kahneman, *Judgment Under Uncertainty: Heuristics and Biases*, 185 SCI. 1124 (1974), https://doi.org/10.1126/science.185.4157.1124 [https://perma.cc/9287-A4YL].

[197] *See, e.g.*, Anita L. Allen, *Dismantling the "Black Opticon": Privacy, Race Equity, and Online Data-Protection Reform*, 131 YALE L.J.F. 907, 932 (2022) (noting that "baseline data privacy and the power data privacy confers may be unequally distributed along racial lines in society").

[198] *See id.*

of targeted advertising, since benefited consumers likely have greater resources and political capital.[199] Finally, privacy harms from online advertising may impede ongoing efforts to remediate the digital divide, where lower-income, minority, and marginalized communities are less likely to have broadband Internet access and to engage in activities such as e-commerce and distance learning.[200] People in these communities also suffer disproportionately from disruptions such as the COVID-19 pandemic that make Internet engagement vital for daily life.[201]

In short, even if targeted advertising is socially beneficial on net, that does not diminish the potential need for interventions to protect those consumers who bear its burdens. Next, this Article turns to privacy issues at each stage of the advertising life cycle.

C. Data Gathering

Data gathering can occur via one of two mechanisms: direct collection, or acquisition from a third-party data broker.

1. Collection

Data collection raises a number of concerns. First, commentators raise objections related to market failures for transactions in personal information between a consumer and a site or platform.[202] Users may not have meaningful choice if the price of entry to a key application is

[199] *See* Timur Kuran & Cass R. Sunstein, *Availability Cascades and Risk Regulation*, 51 STAN. L. REV. 683, 704 (1999).

[200] *See* Vardhmaan Jain, Mahmoud Al Rifai, Michelle T. Lee, Ankur Kalra, Laura A. Petersen, Elizabeth M. Vaughan, Nathan D. Wong, Christie M. Ballantyne & Salim S. Virani, *Racial and Geographic Disparities in Internet Use in the U.S. Among Patients with Hypertension or Diabetes: Implications for Telehealth in the Era of COVID-19*, 44 DIABETES CARE e15, e15 (2021); Qinyun Lin, Susan Paykin, Dylan Halpern, Aresha Martinez-Cardoso & Marynia Kolak, *Assessment of Structural Barriers and Racial Group Disparities of COVID-19 Mortality with Spatial Analysis*, 5 JAMA NETWORK OPEN 1, 1-2 (2022); Sara Atske & Andrew Perrin, *Home Broadband Adoption, Computer Ownership Vary by Race, Ethnicity in the U.S.*, PEW RSCH. CTR. (July 16, 2021), https://www.pewresearch.org/fact-tank/2021/07/16/home-broadband-adoption-computer-ownership-vary-by-race-ethnicity-in-the-u-s/ [https://perma.cc/WM7Q-4DBQ].

[201] *See* sources cited *supra* note 200.

[202] *See* Strandburg, *supra* note 30, at 95 (stating "[t]here is no functioning market based on exchanges of personal information for access to online products and services").

revelation of personal information.[203] For many job seekers, access to LinkedIn is a necessity for mounting an adequate search.[204]

Second, there may be barriers, such as network effects, that make it difficult to switch away from an app or site if one decides that its privacy practices are no longer tolerable.[205] It is possible, with difficulty, to extract one's data from Facebook, but it is practically impossible to convince all of one's friends and contacts to join a migration to a different social network.[206]

Third, information asymmetries may impede consumers from evaluating proposed bargains, since there is no thick market for personal data, especially since most exchanges are directly for services rather than for intermediate stored value mechanisms such as currencies.[207] We buy Facebook access by sharing information rather than paying cash.[208] Consumers face risks from both over and underestimating the value of their data: they may share valuable information too readily, or forgo beneficial transactions due to an unrealistic view of what their profile is worth.[209]

Fourth, collecting certain data may be normatively problematic because the consumer may be especially vulnerable or the information may be particularly sensitive. The former concern is illustrated by the restrictions on data collection from children under thirteen in the United States imposed by the Children's Online Privacy Protection Act ("COPPA").[210] The latter is demonstrated by the European Union's

---

[203] *See* Rothchild, *supra* note 18, at 183-84.

[204] *See* Marcia Silva, *5 Reasons Why You Really Should Have a LinkedIn Profile*, HIGHER EDUC. RECRUITMENT CONSORTIUM (Dec. 5, 2022), https://www.hercjobs.org/5-reasons-why-you-really-should-have-a-linkedin-profile/ [https://perma.cc/9J7U-WKNX].

[205] *See* Nikolas Guggenberger, *Essential Platforms*, 24 STAN. TECH. L. REV. 238, 243-44 (2021); Yafit Lev-Aretz & Katherine J. Strandburg, *Privacy Regulation and Innovation Policy*, 22 YALE J.L. & TECH. 256, 283-84 (2020).

[206] *See* Lev-Aretz & Strandburg, *supra* note 205, at 289.

[207] *See* Edward J. Janger, *Muddy Property: Generating and Protecting Information Privacy Norms in Bankruptcy*, 44 WM. & MARY L. REV. 1801, 1849 (2003).

[208] *See* Lev-Aretz & Strandburg, *supra* note 205, at 286-87.

[209] *See id.*

[210] *See* Eldar Haber, *The Internet of Children: Protecting Children's Privacy in a Hyper-Connected World*, 2020 U. ILL. L. REV. 1209, 1211 (2020). *But see* danah boyd, Eszter Hargittai, Jason Schultz & John Palfrey, *Why Parents Help Their Children Lie to Facebook*

limits on gathering sensitive demographic characteristics[211] and also by the ongoing debate regarding re-identification attacks on datasets that can reveal such information.[212] Compiling this information is akin to a per se privacy violation.

Lastly, collection of consumer data online is governed primarily by a site or app's privacy policy. Users rarely, if ever, read such policies, and are unlikely to understand the provisions even if they do.[213] The practical problems encountered with the European Union's directive on Web site cookies is a cogent example: while online entities must notify consumers of their cookie practices, most users immediately assent without more.[214] While the Federal Trade Commission has begun to impose substantive constraints on privacy policies,[215] the Commission's enforcement resources are limited.[216] It is difficult if not impossible for consumers to assess whether an app or site abides by its privacy policies, which undercuts private enforcement.[217]

About Age: Unintended Consequences of the Children's Online Privacy Protection Act, 16 FIRST MONDAY 1, 11 (Oct. 31, 2011), https://doi.org/10.5210/fm.v16i11.3850 [https://perma.cc/F7NZ-NLYZ]; Zahra Takhshid, *Children's Digital Privacy and the Case Against Parental Consent*, 101 TEX. L. REV. 1417, 1417 (2023).

[211] *See* Catherine Stupp, *EU Court Expands Definition of Sensitive Data, Prompting Legal Concerns for Companies*, WALL ST. J. (Aug. 10, 2022), https://www.wsj.com/articles/eu-court-expands-definition-of-sensitive-data-prompting-legal-concerns-for-companies-11660123800.

[212] *See* Latanya Sweeney, *k-Anonymity: A Model for Protecting Privacy*, 10 INT'L J. ON UNCERTAINTY, FUZZINESS & KNOWLEDGE-BASED SYS. 557, 557 (2002). *But see* Jane Yakowitz, *Tragedy of the Data Commons*, 25 HARV. J.L. & TECH. 1, 4 (2011).

[213] *See* Lev-Aretz & Strandburg, *supra* note 205, at 284-86.

[214] *See* James Vincent, *The EU Is Trying to Fix Its Abysmal Cookie Consent Policy*, VERGE (May 7, 2020, 3:00 AM), https://www.theverge.com/2020/5/7/21250300/eu-cookie-consent-policy-updated-guidelines-cookie-wall [https://perma.cc/N25P-5GYP].

[215] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 583 (2014). *But see* Justin (Gus) Hurwitz, *Data Security and the FTC's UnCommon Law*, 101 IOWA L. REV. 955, 955 (2016).

[216] *See* FED. TRADE COMM'N, ANNUAL PERFORMANCE REPORT FOR FISCAL YEAR 2023 AND ANNUAL PERFORMANCE PLAN FOR FISCAL YEARS 2024-2025, at 3, 6 (2023) https://www.ftc.gov/system/files/ftc_gov/pdf/FY-2023-Annual-Performance-Report-and-FY-2024-25-Plan.pdf [https://perma.cc/VNJ3-G9DD] (noting Commission's estimated full-time equivalent workforce at only 1217 employees).

[217] The growing value of data, especially in the aggregate, can push data-gathering entities to use broader or more vague language in privacy policies, allowing them more

2. Acquisition

The acquisition of data from a third party, such as a data broker, raises every concern described above regarding collection, albeit less directly: the existence of a market for this information can create problematic incentives for collection. Plus, there is at least one more privacy risk that arises from purchasing consumer data: the buyer may be less able (or, perhaps, willing) to verify the accuracy of the information.[218] Harm from inaccurate consumer information arises principally when that data is used, but transactions create the risk initially.[219] Errors are common in consumer credit reports, for example, even though reports are regulated by the federal Fair Credit Reporting Act[220] and consumers have some ability to correct inaccurate data.[221]

D. Data Storage

Firms must store at least some consumer data to engage in targeted advertising. The value of that data creates at least three privacy concerns from storage: harms occurring from breaches, whether accidental or deliberate; the increasing risk of inaccuracy from conflicts among information as more data is compiled; and incentives to monetize the data in ways that may contravene the data holder's representations.

freedom to operate. Lorrie Faith Cranor, Candice Hoke, Pedro Giovanni Leon & Alyssa Au, *Are They Worth Reading? An In-Depth Analysis of Online Trackers' Privacy Policies*, 11 I/S 324, 325 (2015); Lev-Aretz & Strandburg, *supra* note 205, at 284-86.

[218] *See* Corey Ciocchetti, *Just Click Submit: The Collection, Dissemination, and Tagging of Personally Identifying Information*, 10 VAND. J. ENT. & TECH. L. 553, 581-82 (2008).

[219] *See* Dell Cameron, *How the US Can Stop Data Brokers' Worst Practices — Right Now*, WIRED (Feb. 8, 2023), https://www.wired.com/story/fcra-letter-data-brokers-privacy-regulation/ [https://perma.cc/J3LF-K6FM].

[220] 15 U.S.C. §§ 1681–1681x (2018).

[221] *See* Jonathan Weinberg, *"Know Everything That Can Be Known About Everybody": The Birth of the Credit Report*, 63 VILL. L. REV. 431, 431 (2018); Colin Bradshaw, Note, *Credit Rating Agencies: Regulation and Liability*, 24 LEWIS & CLARK L. REV. 1489, 1497-98 (2020); Ann Carrns, *More Consumers Complain About Errors on Their Credit Reports*, N.Y. TIMES (Oct. 1, 2021), https://www.nytimes.com/2021/02/19/your-money/credit-report-errors.html.

Breaches of data stores containing consumer information are legion.[222] Moreover, the risk of an attack, and a breach of sensitive data, rises as the value of the data that can be obtained increases.[223] Thus, entities such as advertisers face an inescapable dilemma: as the value of their consumer data rises, the likelihood of a cyberattack and the privacy harm from a breach increase as well.

As entities collect more data about consumers from more sources, the risk of a conflict between those sources that leads to inaccurate conclusions — or even to undeserved uncertainty — grows.[224] Credit reports, which have regulatory oversight and mechanisms for error correction, are notoriously rife with incorrect information.[225] Other consumer datasets may well be worse since they are not subject to legal requirements that attempt to ensure accuracy. And data owners have incentives not to open their files for voluntary oversight: the contents may be trade secrets that confer financial advantage;[226] the entity may not want to reveal the extent of its data collection;[227] and the cost of

[222] *See* VERIZON, 2023 DATA BREACH INVESTIGATIONS REPORT 2 (2023), https://www.verizon.com/business/resources/reports/dbir/2023/master-guide/ [https://perma.cc/S78G-R83N]; Chuck Brooks, *Cybersecurity Trends & Statistics for 2023; What You Need to Know*, FORBES (Mar. 14, 2023), https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/ [https://perma.cc/XZ3N-KMJB].

[223] *See* Sharon Shea, *Data Breach Risk Factors, Response Model, Reporting and More*, TECHTARGET (Dec. 17, 2019), https://www.techtarget.com/searchsecurity/feature/Data-breach-risk-factors-response-model-reporting-and-more [https://perma.cc/6DWF-D83S]. The point is akin to Sutton's Law, which captures an apocryphal statement by the notorious criminal Willie Sutton. Supposedly, when asked why he robbed banks, Sutton replied, "That's where the money is." *See* Barbara Mikkelson, *Willie Sutton — 'That's Where the Money Is*,' SNOPES (Sept. 10, 2008), https://www.snopes.com/fact-check/willie-sutton/ [https://perma.cc/U3BE-NXHP].

[224] *See CFPB Takes Action to Address Junk Data in Credit Reports*, CFPB (Oct. 20, 2022), https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-to-address-junk-data-in-credit-reports/ [https://perma.cc/KQR4-DEGG].

[225] *See* sources cited *supra* note 221.

[226] *See* Jenny Colgate, *Why Privacy and Trade Secret Law Are on a Collision Course*, JDSUPRA (Aug. 8, 2023), https://www.jdsupra.com/legalnews/why-privacy-and-trade-secret-law-are-on-6821298/ [https://perma.cc/PK93-EADJ].

[227] *See* Lev-Aretz & Strandburg, *supra* note 205, at 285-86.

correcting mistakes may be greater than the benefits that improved accuracy delivers.[228]

Monetizing stored data is, in many respects, the mirror image of the concerns discussed regarding data acquisition above. If advertisers have incentives to purchase information from sources with questionable collection practices, the opportunity to sell information gathered from such behavior is also a lure. The expansion in the number of data brokers who trade in information that is traditionally subject to regulation, such as under the Fair Credit Reporting Act ("FCRA") and its progeny,[229] but who are able to sidestep oversight likely increases these incentives and risks.[230] Data brokers also gather and transact in consumer data that does not fall under FCRA's regime or any other specific statutory scheme.[231] This raises the twin specters of accurate data gathered (and then transferred) via problematic means, and of inaccurate information learned through either licit or illicit techniques.[232]

---

[228] *See* Corey A. Ciocchetti, *E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors*, 44 AM. BUS. L.J. 55, 64-65 (2007); Richard Hynes, *The Social Costs of Credit Reporting Errors*, 11 J.L. ECON. & POL'Y 329, 330-31 (2015).

[229] 15 U.S.C. §§ 1681–1681x (2018). FCRA was significantly modified by the Fair and Accurate Credit Transactions Act of 2003. Pub. L. No. 108-159, 117 Stat. 1952 (2003). It was again updated by the Credit CARD Act of 2009. Pub. L. No. 111-24, 123 Stat. 1734 (2010).

[230] *See* U.S. DEP'T OF TREASURY, ASSESSING THE IMPACT OF NEW ENTRANT NON-BANK FIRMS ON COMPETITION IN CONSUMER FINANCE MARKETS 80-83 (2022), https://home.treasury.gov/system/files/136/Assessing-the-Impact-of-New-Entrant-Nonbank-Firms.pdf [https://perma.cc/JT77-DV9F]; *Treasury Report: Fintech Requires More Oversight to Prevent Abuses, Protect Consumers*, ABA BANKING J. (Nov. 16, 2022), https://bankingjournal.aba.com/2022/11/treasury-report-fintech-requires-more-oversight-to-prevent-abuses-protect-consumers/ [https://perma.cc/WW7N-YW2C] (contending that report finds "while fintech firms enable new capabilities, they also create new risks related to data privacy and regulatory arbitrage").

[231] *See, e.g.*, William McGeveran, *Disclosure, Endorsement, and Identity in Social Marketing*, 2009 U. ILL. L. REV. 1105.

[232] *See* 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, 284 (2012) (contending that advertisers utilize techniques that impede consumer choice regarding data collection and targeted advertising).

E. Data Use

The point of gathering and storing data for advertising purposes is, ultimately, to advertise. In addition to selecting which content to display to users, though, advertisers may use data to compile a more complete profile of a consumer, to make inferential leaps using statistical techniques such as machine learning, and to transact in the data.[233]

1. Ad Display

The use of consumer data to select an ad targeted to that person is the core activity analyzed in this Article, and this activity raises vital privacy issues.

First, differential selection among consumers may constitute or enable discrimination in the sense that the choice is made on a legally prohibited basis. For example, advertising for a national hotel chain that specifically sought to exclude consumers with a particular racial or ethnic background would violate federal anti-discrimination laws.[234] Not all rationales for distinguishing among potential recipients of advertising are lawful.[235] More troubling, a 2013 study raises questions about whether apparent racial discrimination in online advertising systems is actually reflective of deeper societal problems with such discrimination.[236] Here, discrimination is rooted in privacy because the

---

[233] *See* Solon Barocas & Helen Nissenbaum, *On Notice: The Trouble with Notice and Consent*, 1 PROC. ENGAGING DATA F.: THE FIRST INT'L F. ON APPLICATION & MGMT. PERS. ELEC. INFO. 1 (2009), https://ssrn.com/abstract=2567409.

[234] *See* 42 U.S.C. § 2000a (2018); Elaine Glusac, *Hotels Grapple with Racial Bias*, N.Y. TIMES (Aug. 1, 2018), https://www.nytimes.com/2018/08/01/travel/hotels-diversity-training.html. *But see* Suja A. Thomas, *The Customer Caste: Lawful Discrimination by Public Businesses*, 109 CALIF. L. REV. 141, 143 (2021) (contending that federal judicial precedent has effectively enabled many forms of racial discrimination in places of public accommodation, such as hotels).

[235] *Cf.* Fair Hous. Council v. Roommates.com, 521 F.3d 1157, 1157 (9th Cir. 2008) (finding certain features of Roommates.com site, which sought to match potential renters with owners of available rooms, could potentially violate the federal Fair Housing Act).

[236] *See* Latanya Sweeney, *Discrimination in Online Ad Delivery* 1 (Jan. 28, 2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2208240 [https://perma.cc/WQL9-ZUHU].

practice depends on identifying online consumers by race, or other sensitive characteristics.

Second, advertisers may offer consumers different prices based upon the information they have about each consumer, a practice known to economists as "price discrimination."[237] Individually based pricing raises privacy concerns even when consumers can opt out, as initial prices may be sticky and the underlying motivations for price discrimination may be invidious.[238] For example, some online retailers initially charged different prices based upon a consumer's mobile device operating system, raising concerns that more technologically sophisticated, and perhaps wealthy, consumers might have a price advantage in e-commerce transactions.[239] This is a long-standing tactic: the travel booking site Orbitz displayed listings for more expensive hotels to Apple Mac users relative to Microsoft Windows users in 2012, and Staples engaged in price discrimination based on data about the user's geographical location.[240] Allowing consumers to pay for privacy to thwart or exploit price discrimination, which is a business model for a number of new start-up firms, will also tend to benefit higher-income consumers and magnify price effects for lower-income ones.[241]

Third, consumers often dislike advertising in general and view targeted advertising as particularly noxious.[242] Empirical data on consumer attitudes are mixed and seem to be both context — and

---

[237] *See* Kirsten Martin, *Manipulation, Privacy, and Choice*, 23 N.C. J.L. & TECH. 452, 476-82 (2022).

[238] *See* Irina D. Manta & David S. Olson, *Hello Barbie: First They Will Monitor You, Then They Will Discriminate Against You. Perfectly.*, 67 ALA. L. REV. 135, 155 (2015).

[239] *See* Aniko Hannak, Gary Soeller, David Lazer, Alan Mislove & Christo Wilson, *Measuring Price Discrimination and Steering on E-commerce Web Sites*, 2014 IMC: PROC. CONF. ON INTERNET MEASUREMENT CONF. 305, 305 (2014), https://doi.org/10.1145/2663716.2663744 [https://perma.cc/H3RW-XG4H]; Christo Wilson, *If You Use a Mac or an Android, E-Commerce Sites May Be Charging You More*, WASH. POST (Nov. 3, 2014), https://www.washingtonpost.com/posteverything/wp/2014/11/03/if-you-use-a-mac-or-an-android-e-commerce-sites-may-be-charging-you-more/.

[240] Wilson, *supra* note 239.

[241] *See* Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1377 (2017).

[242] *See* Chris Jay Hoofnagle, Jennifer M. Urban & Su Li, *Privacy and Advertising Mail*, BERKELEY CTR. L. & TECH. 1 (2012), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2183417 [https://perma.cc/9NLS-BFGN].

demographic — specific.[243] Some users, though, undoubtedly see advertising as an invasion of their privacy, especially in its more intrusive forms.[244] Targeted ads may have a "creepiness" factor based on their personalization, especially when they recommend products that touch upon sensitive subjects such as sexuality.[245]

Finally, targeted advertising may generate more substantial worries when it moves beyond the commercial realm, such as with advertising for political candidates or policy issues. Concerns about discrimination, manipulation, and deception are more pressing when they have spillover effects on others. Part of the controversy over online misinformation and fake news surrounding the 2016 U.S. presidential election had to do with what appeared to be deliberate use of advertising, especially on social media platforms, to attempt to tip (or perhaps to actually tip) the outcome of a very close electoral contest.[246] Privacy issues here may be even more worrisome since people have stronger economic incentives

[243] *See id.* at 4; Khim-Yong Goh, Kai-Lung Hui, & I.P.L. Png, *Privacy and Marketing Externalities: Evidence from Do Not Call* (2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1908495 [https://perma.cc/9NLS-BFGN]; Daniel R. Shiman, *The Impact of Firms' Increased Information About Consumers on the Volume and Targeting of Direct Marketing* (1997), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=555646 [https://perma.cc/3MDS-VM2G].

[244] *See* Nik Froehlich, *The Truth in User Privacy and Targeted Ads*, FORBES (Feb. 24, 2022), https://www.forbes.com/sites/forbestechcouncil/2022/02/24/the-truth-in-user-privacy-and-targeted-ads/ [https://perma.cc/5AZV-FZPW].

[245] *See* Nick Bergus, *How I Became Amazon's Pitchman for a 55-Gallon Drum of Personal Lubricant on Facebook*, GAWKER (Feb. 27, 2012), https://www.gawkerarchives.com/5888718/how-i-became-amazons-pitchman-for-a-55-gallon-drum-of-personal-lubricant-on-facebook [https://perma.cc/F3FG-GS52].

[246] *See* German Alvarez, Jaewon Choi & Sharon Strover, *Good News, Bad News: A Sentiment Analysis of the 2016 Election Russian Facebook Ads*, 15 INT'L J. COMM'N 3027, 3032 (2020); Mark Verstraete, Jane R. Bambauer & Derek E. Bambauer, *Identifying and Countering Fake News*, 73 HASTINGS L.J. 821, 825 (2022); Dipayan Ghosh & Ben Scott, *Facebook's New Controversy Shows How Easily Online Political Ads Can Manipulate You*, TIME (Mar. 19, 2018), https://time.com/5197255/facebook-cambridge-analytica-donald-trump-ads-data/ [https://perma.cc/F4DH-ZWJQ]; Richard Gunther, Paul A. Beck & Erik C. Nisbet, *Fake News May Have Contributed To Trump's 2016 Victory* (Mar. 8, 2018), https://www.documentcloud.org/documents/4429952-Fake-News-May-Have-Contributed-to-Trump-s-2016.html [https://perma.cc/KUZ8-DT9Y]; Issie Lapowsky, *How Russian Facebook Ads Divided and Targeted US Voters Before the 2016 Election*, WIRED (Apr. 16, 2018, 9:00 AM), https://www.wired.com/story/russian-facebook-ads-targeted-us-voters-before-2016-election/ [https://perma.cc/96V8-NDPJ].

to make careful purchasing decisions than they do to make careful political ones: a consumer internalizes most of the costs and benefits of a purchase, but usually only a scant amount of the costs and benefits associated with a politician or policy.[247] And, privacy problems may be more intractable with targeted political advertising, which is protected in large measure by the First Amendment[248] and which is difficult to remediate, since re-running an election is nearly impossible in the United States.[249]

2. Profiling

One significant privacy concern is that advertisers will amass a sizeable, ever-growing dossier of information on individual consumers.[250] There are at least two aspects to this issue. One is the "connect the dots" problem: consumers may be willing to reveal discrete pieces of information for one transaction or to one entity, but only on the assumption that those individual data remain separated legally or practically.[251] For example, a consumer might be willing to reveal their employer to LinkedIn and their health status to their pharmacy, but might not be willing to reveal that combined information to either site or to anyone else.

Another aspect is that profiles may be attractive to actors outside of advertising. Government entities may be interested in obtaining profiles of individual consumers, either through market transactions or

[247] *See* Michael D. Gilbert, *Single Subject Rules and the Legislative Process*, 67 U. PITT. L. REV. 803, 844-45 (2006); Jerry L. Mashaw, *The Economics of Politics and the Understanding of Public Law*, 65 CHI. KENT L. REV. 123, 127 (1989) (stating "law is to be understood as a set of 'deals' among those self-interested actors who have the positions and resources to deflect public power to the pursuit of their private ends").

[248] *See* United States v. Alvarez, 567 U.S. 709, 751-52 (2012).

[249] *See* Alexandra Alper, *Trump Floats Idea That Fraud Could Lead to Re-Do of November Election*, REUTERS (Aug. 18, 2020, 9:46 AM), https://www.reuters.com/article/us-usa-election-trump-redo/trump-floats-idea-that-fraud-could-lead-to-re-do-of-november-election-idUSKCN25E297.

[250] *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1746 (2010) (describing the "database of ruin").

[251] *See* Carpenter v. United States, 585 U.S. 296, 309-13 (2018); Solove, *supra* note 172, at 508.

through legal process.[252] Law enforcement, for example, may be able to buy data that it cannot acquire directly through methods such as surveillance.[253] Moreover, regimes such as the Privacy Act that constrain the federal government from creating data profiles[254] expressly do not apply to private entities.[255]

3. Inferences

Advertisers may use data to make inferences about consumers — to produce estimates about their characteristics when those traits are not directly available from the data.[256] Even if the inference is accurate, using it could be problematic.[257] For example, if a firm correctly concludes that a user belongs to a particular demographic group or has certain interests, that may enable an advertiser to exclude people with those characteristics.[258] Inferences might also empower advertising that targets vulnerable consumers with misinformation.[259] This would be particularly troubling if the characteristics are ones protected by law, such as race, gender, or national origin. Inferences also highlight the shortcomings of targeted advertising regulation that relies on restrictions of sensitive data: AI techniques such as machine learning readily circumvent these constraints.[260]

---

[252] *See* Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 104 (2014).

[253] *See* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. 595, 595 (2004).

[254] *See* 5 U.S.C. § 552a (2018).

[255] *See id.* The Privacy Act applies only to federal agencies. *Id.* § 551(1).

[256] *See* Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 NW. U. L. REV. 357, 361-63 (2022).

[257] *See* Sandra Wachter, *Affinity Profiling and Discrimination by Association in Online Behavioral Advertising*, 35 BERKELEY TECH. L.J. 367, 370 (2020).

[258] *See* Jinyan Zang, *Solving the Problem of Racially Discriminatory Advertising on Facebook*, BROOKINGS (Oct. 19, 2021), https://www.brookings.edu/articles/solving-the-problem-of-racially-discriminatory-advertising-on-facebook/ [https://perma.cc/J6DN-YNLL].

[259] *Id.*

[260] *See* Anya E.R. Prince & Daniel Schwarcz, *Proxy Discrimination in the Age of Artificial Intelligence and Big Data*, 105 IOWA L. REV. 1257, 1273-76 (2020).

4. Transactions

Entities that hold consumer data may share it for at least three reasons. The first is to enable related organizations, such as subsidiaries, to advertise effectively. This is the internalized equivalent of a market transaction, although typically it will not involve the actual exchange of funds.[261] All of the privacy concerns explicated in this Part related to use and storage apply to the related organization as well.

The second reason for sharing is to monetize the data. This raises the concerns described above for data storage.

The last reason is that the data controller may share the information for non-pecuniary reasons — in particular, providing it to the government.[262] While such sharing may be lawful, it may nonetheless raise privacy concerns, such as about the increasing power of the surveillance state.[263] For example, Amazon shared video data from its Ring smart doorbells with law enforcement without the particularized consent of the owners of those doorbells.[264] Amazon stated that it shares Ring information with law enforcement only when the company makes "a good-faith determination that there was an imminent danger of death or serious physical injury to a person requiring disclosure of information without delay."[265] However, legislators and civil society organizations are concerned about Amazon's practices because, as reported by the Electronic Frontier Foundation, the Los Angeles Police Department

[261] This is simply Ronald Coase's point: organizations may internalize or externalize functions based on cost or efficiency. While there might be substantive differences between transactions within a firm or set of related firms versus external actors, such as the level of contractually specified precautions, it is likely that these substantive measures are implemented through alternative means, such as internal organizational norms or higher-level agreements such as ones that specify ownership. *See generally* Ronald H. Coase, *The Nature of the Firm*, 4 ECONOMICA 386, 387-88 (1937).

[262] *See* Joshua A.T. Fairfield & Erik Luna, *Digital Innocence*, 99 CORNELL L. REV. 981, 1033 (2014).

[263] *See* Kimberly N. Brown, *Outsourcing, Data Insourcing, and the Irrelevant Constitution*, 49 GA. L. REV. 607, 610-13 (2015).

[264] *See* Alfred Ng, *Amazon Gave Ring Videos to Police Without Owners' Permission*, POLITICO (July 13, 2022), https://www.politico.com/news/2022/07/13/amazon-gave-ring-videos-to-police-without-owners-permission-00045513 (quoting Brian Huseman, Amazon's vice president of public policy).

[265] *Id.*

specifically requested Ring footage related to Black Lives Matter protests.[266] Under pressure, Amazon suspended law enforcement access to Ring data in late January 2024.[267] The larger point is that data is readily re-purposed, both within the private sector and for government.

IV. THE REGULATORS

The laws governing targeted advertising in the United States are a complex patchwork. Some apply to all advertisers, such as the prohibition on unfair or deceptive acts or practices under the Federal Trade Commission Act,[268] and some are industry or medium-specific, such as the CAN SPAM Act[269] or FDA regulations[270] Certain rules affect only specific types of content, such as material about political campaigns, that may not seem like advertising at all on first impression. This Part briefly summarizes the major legal regimes and regulators that define the boundaries for permissible targeted advertising. It also examines *anti*-regulatory doctrines, such as the First Amendment, which constrain regulation of advertising.[271]

A. Federal Trade Commission

The Federal Trade Commission ("FTC") is arguably America's most powerful advertising regulator by dint of the fact that it is the de facto national privacy regulator.[272] The Commission's remit under its Section 5 authority provides the agency with broad, wide-ranging powers to

[266] *See* Matthew Guariglia & Dave Maass, *LAPD Requested Ring Footage of Black Lives Matter Protests*, ELEC. FRONTIER FOUND. (Feb. 16, 2021), https://www.eff.org/deeplinks/2021/02/lapd-requested-ring-footage-black-lives-matter-protests [https://perma.cc/B8KB-XGXV].

[267] *See* Annie Palmer, *Amazon's Ring Will Stop Allowing Police to Request Doorbell Video Footage from Users*, CNBC (Jan. 24, 2024), https://www.cnbc.com/2024/01/24/amazons-ring-will-stop-letting-police-request-doorbell-video-footage.html [https://perma.cc/EB3N-PHXN].

[268] 15 U.S.C. § 45(a)(1).

[269] *Id.* §§ 7701.

[270] 21 C.F.R. § 202.1 (2024).

[271] *See* Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 564 (1980).

[272] *See* Solove & Hartzog, *supra* note 215, at 585-86.

police unfair and deceptive practices, including in advertising.[273] And, the FTC's dual role as enforcer and judge (at least in the first instance) gives it considerable sway over entities in the advertising ecosystem, especially since its enforcement actions nearly always end in settlements.[274] Finally, the FTC is not limited to particular economic sectors or industries; it has wide-ranging authority enabling the Commission to pursue almost any advertising-based violation. In recent years, the FTC has launched a number of investigations based on advertising, leading to rapid settlements with its targets. For example, the FTC pursued Edmodo, an information technology firm in the education market, for obtaining and using data about children for advertising purposes.[275] Edmodo settled the litigation quickly.[276]

As an advertising regulator, the FTC wields considerable power, especially since its decisions about whether to commence — or refrain from — an investigation are unreviewable exercises of the agency's discretion.[277] Although the Commission often considers input from competitors and consumers, it does not need any other party's approval to begin enforcement. The near-unbroken pattern of settlements in its Section 5 privacy cases means that courts can only rarely evaluate whether the FTC's actions are sufficiently grounded in fact and law.[278] The Commission has two distinct advantages: it can not only select privacy cases that maximize the efficacy of its limited resources, it can pick ones that optimize the agency's chances of success (which, in turn, breeds further success based upon the enforcer's reputation for winning).[279] The FTC is thus the regulator with the broadest

[273] *See* 15 U.S.C. § 45(a)(1); Press Release, FTC, FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising (Feb. 1, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising [https://perma.cc/ZZ9B-2G74].

[274] *See* sources cited *supra* note 215.

[275] *See* Stipulated Order for Permanent Injunction and Civil Penalty Judgment at 2, United States v. Edmodo, LLC, No. 23-cv-2495 (N.D. Cal. June 27, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/Edmodo-Dkt15%28Order%20Signed%20by%20the%20Court%29.pdf [https://perma.cc/F3HU-J75R].

[276] *See id.*

[277] *See* Hurwitz, *supra* note 215, at 984.

[278] *See id.*

[279] *See* sources cited *supra* note 215.

jurisdiction, and the greatest clout, for targeted advertising in the United States.[280]

B. Food and Drug Administration

The Food and Drug Administration ("FDA") has a declining but still meaningful role in regulating advertising, especially that which is targeted at consumers. Until 1997, the FDA took the position that it had statutory authority under the Food, Drug & Cosmetic Act ("FDCA") to regulate advertising by manufacturers and distributors of prescription drugs.[281] Pharmaceutical firms were free to advertise to physicians, such as via ads in medical journals, but appeals aimed at consumers were not permitted.[282] In the 1980s and 1990s, though, two factors began to undermine the FDA position. First, drug firms correctly concluded that direct-to-consumer advertising could both provide patients with additional information and also increase pharmaceutical company profits.[283] Second, the evolution of First Amendment doctrine in the courts, particularly regarding commercial speech, suggested that a free speech challenge to the FDA's ban might succeed, potentially stripping the agency of any ability to constrain advertising that was not plainly false or misleading.[284] The agency executed a strategic retreat, issuing

[280] *See* A. Michael Froomkin, Phillip J. Arencibia & P. Zak Colangelo-Trenner, *Safety as Privacy*, 64 ARIZ. L. REV. 921, 938-39 (2022).

[281] *See* Robin Feldman, *Advertising Medicine: Selling the Cure*, 26 STAN. TECH. L. REV. 1, 7-14 (2023).

[282] *Id.*; *see also* United States v. Caronia, 703 F.3d 149, 152 (2d Cir. 2012) (overturning conviction against pharmaceutical company sales consultant for off-label promotion of prescription drug on First Amendment grounds).

[283] *See* Miguel J. Franquiz & Amy L. McGuire, *Direct-to-Consumer Drug Advertisement and Prescribing Practices: Evidence Review and Practical Guidance for Clinicians*, 36 J. GEN. INTERNAL MED. 1390, 1392 (2020) (finding increase in both appropriate and inappropriate prescribing due to direct-to-consumer advertising); Neeraj Sood, *Should the Government Restrict Direct-to-Consumer Prescription Drug Advertising? Six Takeaways on Their Effects*, EVIDENCE BASE (Mar. 23, 2023), https://healthpolicy.usc.edu/article/should-the-government-restrict-direct-to-consumer-prescription-drug-advertising-six-takeaways-from-research-on-the-effects-of-prescription-drug-advertising/ [https://perma.cc/BT8K-GPL5].

[284] *See* Kathleen M. Sullivan, *Cheap Spirits, Cigarettes, and Free Speech: The Implications of* 44 Liquormart, 1996 SUP. CT. REV. 123, 124 (noting that "[i]n recent terms . . . the Court has granted repeated victories to advertisers in First Amendment challenges"); *id.* at 147-48 (describing "intermediate scrutiny [of commercial speech such as advertising]

new regulations in 1997 that focused on the content of advertising messages rather than their intended audience.[285] Direct-to-consumer ("DTC") messaging has increased dramatically, and there is vigorous debate among analysts and scholars as to the overall effects of the shift.[286] The FDA still has oversight authority for advertising, but the scope of that authority has diminished considerably over time.

C. CAN SPAM

In 2003, Congress passed (and President George W. Bush signed into law) the CAN SPAM Act, which imposes restrictions on e-mail messages that have the primary purpose of commercial advertisement or promotion of a commercial product or service.[287] CAN SPAM's scope is narrow relative to laws regulating e-mail advertising in other countries, but that coverage was a deliberate policy choice: advertisers, most notably the Direct Marketing Association (now part of the Association of National Advertisers), were concerned about the proliferation of state-level statutes regulating spam. Advertisers were especially worried about state laws that posed mutually incompatible requirements.[288] CAN SPAM's remit was thus limited in important ways: the law imposed an opt-out regime, enabling advertisers to communicate via unsolicited e-mail until a recipient indicated they did not want to receive messages;[289] it exempted e-mail related to a transaction between the sender and the recipient;[290] and it pre-empted state laws on the subject except to the extent that they addressed falsity or deception in messages.[291] In addition to relatively narrow subject matter coverage,

under *Central Hudson* is a doctrinal anomaly: intermediate in theory but often fatal in fact").

[285] FOOD & DRUG ADMIN., GUIDANCE FOR INDUSTRY: CONSUMER-DIRECTED BROADCAST ADVERTISEMENTS 1 (1999); Feldman, *supra* note 281, at 7.

[286] *See* Feldman, *supra* note 281, at 13-14.

[287] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003).

[288] *See* Derek E. Bambauer, *Solving the Inbox Paradox: An Information-Based Policy Approach to Unsolicited E-mail Advertising*, 10 VA. J.L. & TECH. 1, 31 (2005).

[289] 15 U.S.C. § 7704(a)(4).

[290] *Id.* § 7702(2)(B).

[291] *Id.* § 7707(b)(1).

CAN SPAM scattered enforcement authority across ten different federal entities along with each state's insurance authority.[292] Lastly, the act sidelined more controversial proposals, such as a Do-Not-Email list[293] or qui tam-style rewards for private enforcers,[294] in favor of studies by the FTC on these topics. The Commission, unsurprisingly, eventually recommended against implementing these measures.[295]

D. Children's Online Privacy Protection Act

In 1998, Congress addressed concerns about Internet firms' data collection practices regarding minors with the Children's Online Privacy Protection Act ("COPPA").[296] COPPA forbade online services from collecting personal information from children under the age of thirteen unless the service provided a privacy policy specifying what information it collected, how it used that information, and what disclosures it made of the information.[297] Online firms would also have to furnish to a child's parent, upon request, a description of the specific types of personal information collected about that child; to abide by the parent's refusal to permit continued use or maintenance of that information, as well as any further collection; and to enable the parent to obtain information held by the firm about the child.[298] Services were also required to establish and maintain reasonable precautions to

[292] *Id.* § 7706(b).

[293] *Id.* § 7708.

[294] *Id.* § 7710.

[295] FTC, A CAN-SPAM INFORMANT REWARD SYSTEM: A REPORT TO CONGRESS 28 (2004), https://www.ftc.gov/sites/default/files/documents/reports/can-spam-informant-reward-system-federal-trade-commission-report-congressexpert-reports/040916rewardsysrpt.pdf [https://perma.cc/X3YD-YQDK]; FTC, NATIONAL DO NOT EMAIL REGISTRY: A REPORT TO CONGRESS 37 (June 2004), https://www.ftc.gov/sites/default/files/documents/reports/can-spam-act-2003-national-do-not-email-registy-federal-trade-commission-report-congress/report.pdf [https://perma.cc/6YUZ-RKGF].

[296] Children's Online Privacy Protection, Pub. L. No. 105-277, 112 STAT. 2681 (2000) (codified at 15 U.S.C. §§ 6501–6506).

[297] 15 U.S.C. §§ 6502(a)(1), (b)(1). Formally, COPPA mandated that the FTC promulgate regulations implementing these requirements, which it did in April 2000. The FTC updated its COPPA Rule in 2013. Children's Online Privacy Protection Rule, 78 FED. REG. 3972 (Jan. 17, 2013) (updating 16 C.F.R. § 312).

[298] 15 U.S.C. § 6502(b)(1)(B).

maintain the confidentiality, security, and integrity of personal information about children.[299] Thus, even without a comprehensive data collection governance regime, the federal government implemented a system of more limited applicability to address concerns about the online use and disclosure of personal information of children under thirteen, such as in advertising.

E. State Statutes

States have begun to regulate online advertising in the past few years, albeit indirectly via data privacy laws. Twenty states now have consumer privacy regimes.[300] There are two basic models: California, which has a broader scheme including rulemaking by a new administrative entity, the California Privacy Protection Agency; and Virginia, which is the baseline for the other states.[301] The International Association of Privacy Professionals categorizes the Virginia regimes into a set of core obligations adopted by Virginia and four other states,[302] a set of more expansive substantive obligations enacted by five states,[303] and a set of

[299] *Id.* §6502(b)(1)(D).

[300] *See Which States Have Consumer Data Privacy Laws?*, BLOOMBERG L. (Sept. 10, 2024), https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker/; [https://perma.cc/Q3SU-HRMZ].

[301] *See Models of State Privacy Legislation*, BSA (Sept. 12, 2023), https://www.bsa.org/files/policy-filings/09122023privacyleg.pdf [https://perma.cc/4EDY-EJMW] [hereinafter *BSA Chart*].

[302] *See* Joseph Duball, *Nuances Highlight New Jersey's Comprehensive Privacy Bill*, INT'L ASS'N OF PRIV. PROS. (Jan. 10, 2024), https://iapp.org/news/a/nuances-highlight-new-jerseys-comprehensive-privacy-bill/ [https://perma.cc/B7UG-54KD]. The IAPP suggests that the New Jersey law may represent a hybrid approach between the California and Virginia models. Olga Medina, *US States Leverage Existing Models of Privacy Legislation*, INT'L ASS'N OF PRIV. PROS. (Sept. 13, 2023), https://iapp.org/news/a/u-s-states-leverage-existing-models-of-privacy-legislation/ [https://perma.cc/JCR2-2RRX]. The states are Florida, Indiana, Tennessee, Texas, and Virginia. Note that New Jersey's privacy legislation was enacted on January 16, 2024, after this Article was written. *See generally New Jersey's Comprehensive Privacy Bill Signed into Law*, INT'L ASS'N OF PRIV. PROS. (Jan. 17, 2024), https://iapp.org/news/a/new-jerseys-comprehensive-privacy-bill-signed-into-law/ [https://perma.cc/8P2J-KCVB].

[303] Medina, *supra* note 302 (The states are Colorado, Connecticut, Delaware, Montana, and Oregon).

less expansive substantive obligations signed into law in two states.[304] Thirteen states (all except Iowa) allow consumers to opt out of targeted advertising; twelve states (all except Iowa and Utah) allow one to opt out of profiling.[305] All fourteen states allow consumers to opt out of sales of their data.[306] Only Colorado, Delaware, and Oregon require non-profit organizations (in addition to for-profit businesses) to follow their mandates.[307] Every state authorizes its attorney general to enforce its data privacy rules — none enables private actors to do so.[308] Although California's model differs significantly from the other thirteen states with data privacy laws, its decision to enact privacy legislation was plainly the catalyst for the emergence of individual states as substantive privacy regulators.[309]

F. The European Union

While the European Union cannot formally regulate how American entities advertise to U.S. citizens, its legal rules have a gravitational effect on targeted advertising in the U.S. for at least two reasons. First, organizations that also control or process data about EU citizens must comply with relevant EU regimes, most prominently the General Data

[304] *Id.* The states are Iowa and Utah. The IAPP's classification scheme is internally inconsistent. An overview written in September 2023 includes Florida's Digital Bill of Rights as based on the Virginia model. *Id.* However, the organization's U.S. State Privacy Legislation Tracker, updated in February 2024, excludes the Florida legislation. Andrew Folks, *US State Privacy Legislation Tracker*, INT'L ASS'N OF PRIV. PROS., https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ (last updated Feb. 9, 2024) [https://perma.cc/ZXC5-G5D8] (noting that "[i]f a bill does not appear on the tracker, it does not qualify due to its scope, coverage, rights or purpose"). BSA (formerly the Business Software Alliance) states that the Florida law's "coverage thresholds are higher than those [of other states] and apply to a more limited set of companies." *BSA Chart*, *supra* note 301. This may explain the IAPP divergence.

[305] *See BSA Chart*, *supra* note 301. New Jersey's recently enacted legislation includes both opt-outs. *See* S. 332, 220th Leg. (N.J. 2024), https://www.njleg.state.nj.us/bill-search/2022/S332 [https://perma.cc/5GLG-5RP6].

[306] *See BSA Chart*, *supra* note 301.

[307] *Id.*

[308] *Id.*

[309] *See* Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1736-40 (2021).

Protection Regulation.[310] That requirement may influence how they interact with American citizens and their data as well, if only because of the cost and complexity of managing two sets of rules internally.[311] Second, the "Brussels Effect" of EU rules on American ones means that regulations such as the GDPR may be leading indicators of how U.S. law will handle online privacy issues.[312] Complying with the GDPR and its kin may simply save time.

However, commentators generally agree that the GDPR's rules on targeted advertising have not been widely or consistently enforced.[313] There are high-profile exceptions, such as the fifty million euro fine imposed on Google by the French data protection authority CNIL for lack of a proper basis for personalized advertising, but thus far targeted advertising has mostly escaped EU regulatory enforcement measures.[314] The EU tacitly agrees that the GDPR and related regulation have not been sufficient because it has proposed a series of additional measures, including ones on the use of artificial intelligence for targeted advertising and for personalization in political ads, as responses.[315] Assuming that the EU does increase the efficacy of its targeted advertising regulation, American firms will likely move towards compliance with Europe's rules, both as a cost-saving measure and perhaps as a leading indicator of coming changes in U.S. advertising regulation.

---

[310] *See* 2016 O.J. (L 119) 679; 2018 O.J. (L 127) 673; Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1, 18 (2012) (describing technical nondivisibility, where the EU "forces companies like Google to amend their data storage and other business practices to conform to European privacy standards [because firms are] [u]nable to . . . isolate data collection for the EU for technical reasons").

[311] Bradford, *supra* note 310, at 64.

[312] *See id.* at 3. *But see* Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365, 411-31 (2019) (arguing that there is a "D.C. Effect" whereby American privacy norms and laws influence EU regulation).

[313] *See* Zard & Sears, *supra* note 63, at 802-04.

[314] *See* W. Gregory Voss & Hugues Bouthinon-Dumas, *EU General Data Protection Regulation Sanctions in Theory and in Practice*, 37 SANTA CLARA HIGH TECH. L.J. 1, 79-83 (2021).

[315] *See* Zard & Sears, *supra* note 63, at 803-805.

G. Anti-Regulation

This Section explores the legal doctrines that limit the regulatory regimes described above, which are the most important aspects of the targeted regulation anti-canon.

1. First Amendment

The First Amendment to the United States Constitution is, at least beginning in the latter half of the twentieth century, the strongest guarantee that advertisers may communicate messages to the public.[316] For much of U.S. history, commercial speech was treated as outside free speech protection entirely.[317] However, the Supreme Court eventually moved commercial speech inside the ken of protected speech[318] and has arguably increased protection for it since the advent of the Roberts Court.[319] The practical import of this doctrinal shift is that U.S. governments are not free to regulate advertising content based purely on whim or arbitrary reasoning. Rather, legal rules must meet four criteria. First, to receive protection, the commercial speech at issue must "concern lawful activity and not be misleading."[320] If it is, then the government interest advanced as a justification for the regulation must be substantial.[321] Finally, the regulation must both advance that particular government interest and must be no more extensive than necessary to do so.[322] This means that governments may not ban commercial communication due to fears that consumers will shop based

[316] Sorrell v. IMS Health Inc., 564 U.S. 552, 557 (2011); Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557, 569-72 (1980); Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, 425 U.S. 748, 770-73 (1976).

[317] *See* Valentine v. Chrestensen, 316 U.S. 52, 54 (1942); Jane R. Bambauer & Derek E. Bambauer, *Information Libertarianism*, 105 CAL. L. REV. 335, 343 (2017).

[318] *Cent. Hudson*, 447 U.S. at 571-72.

[319] *See* Enrique Armijo, *Faint-Hearted First Amendment Lochnerism*, 100 B.U. L. REV. 1377, 1380 (2020); Enrique Armijo, Reed v. Town of Gilbert: *Relax, Everybody*, 58 B.C. L. REV. 65, 81 (2017); Genevieve Lakier, *Reed v Town of Gilbert, Arizona, and the Rise of the Anticlassificatory First Amendment*, 2016 SUP. CT. REV. 233, 235-36.

[320] *Cent. Hudson*, 447 U.S. at 566.

[321] *Id.*

[322] *Id.*

upon price rather than upon expert service from vendors,[323] or that they will opt for higher-proof alcoholic beverages rather than lower-proof ones.[324]

The First Amendment thus disempowers governments rather than provides them with a source of authority. It reflects faith in the power of the marketplace of ideas: that consumers, provided with truthful information about the products and services that interest them, will act in their own best interests.[325] And, it leaves copious room for state and federal governments to prohibit advertising that lies to or misleads consumers.[326] The modern commercial speech doctrine strikes a tenuous middle ground: it authorizes government to forbid false or misleading advertising, but not that which conveys truthful information. This constraint limits regulation of truthful targeted advertising.

2. State Constitutional Provisions

State-level constitutional protections for free speech can also play a role in regulating advertising, albeit one with narrower scope than federal doctrine.[327] For example, California's constitution provides free speech safeguards that are widely perceived as stronger — more protective of expression — than the federal First Amendment.[328] Indeed, Article One, Section Two of California's Constitution provides affirmative rights to speakers engaged in political advertising, at least in the context of multi-store shopping malls.[329] Although the California courts have both expanded and contracted the scope of this free expression right over time, it remains broader than any federal

[323] Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 768 (1976).

[324] 44 Liquormart, Inc. v. Rhode Island, 517 U.S. 484, 489 (1996).

[325] *See* Joseph Blocher, *Institutions in the Marketplace of Ideas*, 57 DUKE L.J. 821, 829-38 (2008).

[326] *See 44 Liquormart*, 517 U.S. at 498-99.

[327] *See* Genevieve Lakier, *The Non-First Amendment Law of Freedom of Speech*, 134 HARV. L. REV. 2299, 2302 (2021).

[328] *Id.*

[329] Pruneyard Shopping Ctr. v. Robins, 447 U.S. 74, 79-88 (1980); Robins v. Pruneyard Shopping Ctr., 23 Cal. 3d 899, 910 (1979).

equivalent (which is limited to, at most, access to property whose operation "is essentially a public function," such as a town owned by a private company).[330] However, such protections run no further than California's jurisdiction in its state courts; other states have split upon whether to follow the Golden State's approach to free expression.[331]

V. THE REFORM

Targeted advertising has been highly politically salient in the past several years, making it the target of an array of proposals for regulatory reform. The candidates range from preliminary inquiries[332] to structural interventions in industry[333] to conduct prohibitions[334] to outright bans on using personal information.[335] These are layered on top of (or may pre-empt) a burgeoning set of state advertising regulations focused on security and privacy.[336] Thus far, however, none of the federal proposals has been adopted by Congress, and the likelihood of passage for comprehensive legislation in a politically divided government with a looming presidential election is low.

Given the political climate, along with the practical challenges of designing a successful intervention in a complex, evolving industry, this Article proposes a more targeted reform that can serve as a proof of concept for further reform. It relies upon a co-regulatory model that focuses on three problems that are currently under-addressed by existing regulation: transactions in personally identifiable

330 Marsh v. Alabama, 326 U.S. 501, 506 (1946).

331 *See, e.g.*, Brady C. Williamson & James A. Friedman, *State Constitutions: The Shopping Mall Cases*, 1998 WIS. L. REV. 883, 886-87.

332 *See* Trade Regulation Rule on Commercial Surveillance and Data Security, 87 FED. REG. 51273 (Aug. 22, 2022).

333 *See, e.g.*, Competition and Transparency in Digital Advertising Act, S. 4258, 117th Cong. (2022).

334 *See, e.g.*, American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

335 Banning Surveillance Advertising Act of 2022, H.R. 6416, 117th Cong. (2022).

336 *See, e.g.*, CAL. CIV. CODE § 1798.100 (2023); UTAH CODE ANN. § 13-61-101 (2023); VA. CODE ANN. § 59.1-575 (2023); *see also* Clark, *supra* note 19; Alfred Ng, *The Raucous Battle over Americans' Online Privacy Is Landing on States*, POLITICO (Feb. 22, 2023), https://www.politico.com/news/2023/02/22/statehouses-privacy-law-cybersecurity-00083775.

information,[337] invasive data collection from consumers,[338] and insecure data storage by industry entities.[339] This reform seeks to generate a set of consensus arrangements, such as delineating best and worst practices,[340] that the FTC would utilize when determining whether to bring a targeted advertising case under its Section 5 authority.[341] The intervention would explicitly sunset after five years unless regulators found it to be effective and re-authorized it. The proposal would affect only enforcement by the FTC initially, although its scope could be expanded if it were to succeed.

This Part proceeds in three sections. First, it sets out some of the challenges for regulation of online advertising. Second, it identifies the problems that the reform proposal would address and why they were selected. Third, it elucidates the specifics of the proposals, their limitations, and prospects for future work.

A. The Challenges of Online Advertising Reform

Personalized advertising has been a popular target for reform proposals in the last several years. To date, these efforts have failed, and the challenges they unsuccessfully confronted persist.

Although some proposed targeted advertising legislation has had bipartisan sponsors,[342] the current political environment is not conducive to large-scale regulatory shifts. While both Republicans and Democrats favor increased regulation of large Internet firms, especially

---

[337] *See* Christopher G. Bradley, *Privacy for Sale: The Law of Transactions in Consumers' Private Data*, 40 YALE J. ON REGUL. 127, 150 (2023).

[338] *See* Camille Cobb, Samuel Sudar, Nicholas Reiter, Richard Anderson, Franziska Roesner & Tadayoshi Kohno, *Computer Security for Data Collection Technologies*, 3 DEV. ENG'G 1, 1 (2018).

[339] *See* Peter C. Ormerod, *A Private Enforcement Remedy for Information Misuse*, 60 B.C. L. REV. 1893, 1894 (2019).

[340] *Cf.* Derek E. Bambauer & Melanie J. Teplinsky, *Shields Up for Software*, LAWFARE (Dec. 19, 2023), https://www.lawfaremedia.org/article/shields-up-for-software [https://perma.cc/M9HV-CT6U] (proposing safe harbor for best practices and strict liability for worst practices as part of software liability regime).

[341] 15 U.S.C. § 45; *see* Hurwitz, *supra* note 215, at 957-58.

[342] *See, e.g.*, AMERICA Act of 2023, S. 1073, 118th Cong. (2023) (listing seven Republican senators and three Democratic senators as co-sponsors).

platforms, they do so for different reasons and to different ends.[343] The 2024 presidential election reduced the likelihood of sustained bipartisan cooperation even on issues where there is some consensus.[344] Furthermore, Internet advertising has not had a dramatic focusing event to concentrate public attention on policy issues associated with the industry.[345]

It is difficult to draft meaningful reform for regulation of targeted advertising. The complexity of both the technological landscape and the business relationships in the Internet advertising business ecosystem complicates oversight.[346] That same complexity increases the information asymmetry between the advertising industry and consumers. It makes meaningful disclosure to consumers hard to achieve.[347] Moreover, the notice-and-consent model that dominates American approaches to privacy regulation is not well-suited to information that consumers voluntarily disclose or inevitably create during online activity.[348] If advertising rules turn on user consent, then they will likely have little effect, because most consumers consent.

In addition, many existing or proposed legal frameworks concentrate heavily on data that discloses sensitive personal characteristics, including

---

[343] *See* AJ Dellinger, *Lawmakers Seek Bipartisan Push on Big Tech Regulation. Voters' Views Indicate Censorship, Content Moderation Could Be Sticking Points*, MORNING CONSULT (Jan. 31, 2023), https://pro.morningconsult.com/instant-intel/lawmakers-seek-bipartisan-push-on-big-tech-regulation [https://perma.cc/84RM-7W6P]; *see also* Gopal Ratnam, *White House, House GOP Take Aim at Big Tech, But See Different Targets*, ROLL CALL, https://rollcall.com/2023/01/17/white-house-house-gop-take-aim-at-big-tech-but-see-different-targets/ (last updated Jan. 17, 2023) [https://perma.cc/8TN4-RJBR].

[344] *See Anti-Predictions*, *supra* note 23.

[345] *See generally* Thomas A. Birkland, *Focusing Events, Mobilization, and Agenda Setting*, 18 J. PUB. POL'Y 53, 53 (1998).

[346] *See* PwC, *supra* note 48, at 8; Megan Graham, *Complexity for Marketers Has Meant Opportunity for Ad Agencies*, WALL ST. J. (Nov. 14, 2022), https://www.wsj.com/articles/complexity-for-marketers-has-meant-opportunity-for-ad-agencies-11668460746.

[347] *See* Ayelet Gordon-Tapiero, Alexandra Wood & Katrina Ligett, *The Case for Establishing a Collective Perspective to Address the Harms of Platform Personalization*, 25 VAND. J. ENT. & TECH. L. 635, 655-56 (2023).

[348] Robert H. Sloan & Richard Warner, *Beyond Notice and Choice: Privacy, Norms, and Consent*, 14 J. HIGH TECH. L. 370, 390-95 (2014). *But see* Daniel Susser, *Notice After Notice-and-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't*, 9 J. INFO. POL'Y 37, 37 (2019).

the European Union General Data Protection Regulation ("GDPR")[349] and some draft U.S. proposals.[350] These rules face obstacles that may prove insuperable. Excluding sensitive data from collection or analysis is unlikely to be effective because many, if not most, sensitive characteristics can be inferred from non-sensitive ones.[351] Machine learning algorithms have proved skillful in finding proxies that replicate sensitive characteristics, and an expanding set of empirical and theoretical research demonstrates that exclusion of sensitive data can worsen the problems that the intervention seeks to remediate.[352] Moreover, certain rationales for using sensitive data, such as to expand employment opportunities for traditionally marginalized groups, are likely to be unobjectionable to most observers.[353] It will be hard to block advertisers from using sensitive data, and it might not be desirable to do so.

Targeted advertising reform is difficult to draft and challenging to pass. The next Section proposes concentrating on a key subset of issues with targeted ads.

B. Regulatory Focus: Data Collection, Storage, and Transactions

This Article concentrates upon three problems with targeted ads because their existence and scope have been elucidated well empirically, and because there are structural factors that make it difficult for current

---

[349] *See What Personal Data Is Considered Sensitive?*, EUR. COMM'N, https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en (last visited Oct. 5, 2024) [https://perma.cc/MU9D-GYWK].

[350] *See, e.g.*, H.R. 6416, 117th Cong. § 2(b)(2) (2022) (prohibiting targeted advertising based on personal information that "identifies an individual as a member of a protected class" or that "act[s] as a reasonably proxy" for such identification); S. 3195, 117th Cong. § 2 (2021) (defining "sensitive data").

[351] *See* sources cited *supra* note 39; Gordon-Tapiero, Wood & Ligett, *supra* note 347, at 641-42.

[352] *See* Damian Clifford, Megan Richardson & Normann Witzleb, *Artificial Intelligence and Sensitive Inferences: New Challenges for Data Protection Laws*, *in* REGULATORY INSIGHTS ON ARTIFICIAL INTELLIGENCE: RESEARCH FOR POLICY 19, 19 (Mark Findlay, Jolyon Ford, Josephine Seoh & Dilan Thampapillai eds., 2021).

[353] *See, e.g.*, H.R. 8152, 117th Cong., § 207(a)(2)(A)(ii) (2022) (allowing collection, processing, or transfer of covered data for purpose of diversifying an applicant, participant, or customer pool).

regulation to mitigate these problems. Ensuring adequate security in the collection and storage of consumer data suffers from a host of regulatory challenges,[354] including information asymmetry, externalities, and technological timidity on the part of regulators (although this last point may be gradually changing).[355] As with data breaches, harms and costs from invasive data collection techniques are well-studied and quantified.[356] Similarly, transactions in personally identifiable consumer information evade regulatory scrutiny, pose challenges of downstream monitoring for providers, and evolve rapidly.[357] The data sold can include highly sensitive information, such as information about one's mental health,[358] military service,[359] and

354 *See* Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011, 1033-40 (2014) [hereinafter Bambauer, *Ghost in the Network*].

355 *See* Tim Starks, *Biden Unveils Cyber Strategy That Takes More Aggressive Regulatory Approach*, WASH. POST (Mar. 2, 2023), https://www.washingtonpost.com/national-security/2023/03/02/cybersecurity-biden/.

356 *See* Aritz Arrate, José González-Cabañas, Ángel Cuevas & Rubén Cuevas, *Malvertising in Facebook: Analysis, Quantification and Solution*, 9 ELECS. 1332, 1332 (2020), https://doi.org/10.3390/electronics9081332 [https://perma.cc/TY2H-8NEG]; *see, e.g.*, IDENTITY THEFT RES. CTR., 2022 DATA BREACH REPORT (2023), https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf [https://perma.cc/2EPL-LLXF]; VERIZON, DATA BREACH INVESTIGATIONS REPORT (2022), https://www.verizon.com/business/resources/Taef/reports/dbir/2022-data-breach-investigations-report-dbir.pdf [https://perma.cc/78YK-3JNW]; *Facts + Statistics: Identity Theft and Cybercrime*, INS. INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited Oct. 5, 2024) [https://perma.cc/9RK5-EP96]. An oft-cited 2015 report by EY for the Internet Advertising Bureau claimed $1.1 billion in cost impact per year from malvertising and related impacts. EY, WHAT IS AN UNTRUSTWORTHY SUPPLY CHAIN COSTING THE US DIGITAL ADVERTISING INDUSTRY? 2 (2015), https://www.iab.com/wp-content/uploads/2015/11/IAB_EY_Report.pdf [https://perma.cc/4ZDE-TYRS].

357 *See* Drew Harwell, *Now for Sale: Data on Your Mental Health*, WASH. POST (Feb. 13, 2023), https://www.washingtonpost.com/technology/2023/02/13/mental-health-data-brokers/; Tatum Hunter, *These Companies Will Pay You for Your Data. Is It a Good Deal?*, WASH. POST (Feb. 6, 2023), https://www.washingtonpost.com/technology/2023/02/06/consumers-paid-money-data/.

358 *See* Harwell, *supra* note 357.

359 *See* Justin Sherman, *Data Brokers Are Advertising Data on U.S. Military Personnel*, LAWFARE (Aug. 23, 2021), https://www.lawfareblog.com/data-brokers-are-advertising-data-us-military-personnel [https://perma.cc/WYW4-8KME].

geographic locations[360] over time.[361] Transactions in such data can be used for legitimate advertising purposes,[362] but they also fuel a wide variety of unlawful behavior[363] or conduct designed to circumvent existing regulatory regimes such as the Fair Credit Reporting Act[364] or the Fourth Amendment.[365] Moreover, disclosure of data such as health-related information is heavily regulated for some information providers, such as health care entities, but unregulated for other sources.[366] That dichotomy likely reflects not a deliberate policy choice but rather the sector-specific model that dominates American data privacy and security law.

Each of these three concerns is under-addressed by current law. Data collection regulations tend to concentrate on what data firms gather, not how they do so.[367] Egregious techniques such as spyware may result

[360] *See id.*; Corin Faife, *Feds Are Tracking Phone Locations with Data Bought from Brokers*, VERGE (July 18, 2022), https://www.theverge.com/2022/7/18/23268592/feds-buying-location-data-brokers-aclu-foia-dhs (https://perma.cc/M96Q-NU9Y); Harwell, *supra* note 357.

[361] These data are far from the most problematic involved in such transactions. The data broker Medbase200 offered for sale lists of what the firm claimed were victims of sexual assault and domestic violence until the executive director of the World Privacy Forum and the Wall Street Journal highlighted its practices. *See* Elizabeth Dwoskin, *Data Broker Removes Rape-Victims List After Journal Inquiry*, WALL ST. J. (Dec. 19, 2013), https://www.wsj.com/articles/BL-DGB-31536; Harwell, *supra* note 357.

[362] *See* Sherman, *supra* note 359.

[363] *See* Cynthia Cole, Brendan Quigley & Natalie Sanders, *Are You a Data Broker? Chances Are High That State and Federal Regulators Think So*, REUTERS (Jan. 20, 2022), https://www.reuters.com/legal/legalindustry/are-you-data-broker-chances-are-high-that-state-federal-regulators-think-so-2022-01-20/.

[364] *See* Cameron, *supra* note 219; Tariq Habash & Mike Saunders, *The Predatory Underworld of Companies That Target Veterans for a Buck*, STUDENT BORROWER PROT. CTR. (Feb. 1, 2019), https://protectborrowers.org/the-predatory-underworld-of-companies-that-target-veterans-for-a-buck/ [https://perma.cc/KS83-9JNA].

[365] *See* Faife, *supra* note 360.

[366] *See* Harwell, *supra* note 357.

[367] *See* Press Release, FTC, FTC Order Will Ban InMarket from Selling Precise Consumer Location Data (Jan. 18, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-will-ban-inmarket-selling-precise-consumer-location-data [https://perma.cc/9PP3-ETC7].

in enforcement, but more subtle mechanisms tend to evade scrutiny.[368] Data storage is more comprehensively regulated, but the regulations simply do not work very well. Breaches are legion.[369] Legal mandates concentrate on how firms respond to breaches, not how to prevent them. Finally, transactions in consumer data are infrequently subject to oversight. On rare occasion, the FTC has intervened to block a transaction that clearly violated an explicit promise from a firm to consumers, but otherwise transactions lack meaningful regulatory governance.[370]

In addition, these three issues are likely to enjoy broader political support, and hence encounter relatively less difficulty in enactment, because they are problems where there is less normative disagreement than other concerns about targeted advertising. For example, people have heterogeneous preferences about what data they are comfortable sharing, even voluntarily.[371] Whatever one's substantive preferences about information disclosure, though, it is likely that one prefers to have companies take sufficient security precautions to protect that data from unauthorized access and use.[372] Similarly, even consumers with divergent views about what information to share with platforms and advertisers are likely to agree that it is unacceptable to use invasive techniques to obtain it. And people with widely divergent political viewpoints probably agree that the current market in information transactions is undesirable if it has adverse effects on members of the military, or people who visit providers of abortion services, or people

[368] *See* Decision and Order at 5, *In re* Support King, LLC., No. C-4756 (F.T.C. Dec. 20, 2021), https://www.ftc.gov/system/files/documents/cases/1923003c4756spyfoneorder.pdf [https://perma.cc/NN8W-XJ62].

[369] *See supra* note 222 and accompanying text.

[370] *See* Press Release, FTC, FTC Announces Settlement with Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations (July 21, 2000), https://www.ftc.gov/news-events/news/press-releases/2000/07/ftc-announces-settlement-bankrupt-website-toysmartcom-regarding-alleged-privacy-policy-violations [https://perma.cc/Y9V8-3PJG].

[371] *See* Hunter, *supra* note 357.

[372] *See* Bambauer, *Privacy Versus Security*, *supra* note 178, at 667.

who patronize firearms dealers.[373] These three regulatory issues are not easy, but they are easier than the alternatives.

Reform advocates could contend that regulation addressing only these three areas is inadequate. That might be true. This Article's proposal is intended as a first step, not a last step. If its proposed intervention is adopted and proves effective, it could be extended to address other risks or harms from targeted advertising. The initial proposal, though, concentrates on areas of relative political consensus, where there is good data to guide policy, as a proof of concept and as a means of measuring how effective a model of collaborative enforcement can be for advertising. The next Section elaborates the proposed intervention.

C. Effective Reform Via Co-Regulation

This Article's proposed intervention is a time-limited trial of a co-regulatory model that concentrates on harms from invasive data collection, insecure data storage, and transactions in personally identifiable information. It addresses the challenges of information asymmetry by drawing upon private information held by advertising industry entities. The reform combines the power of that private information[374] with public enforcement by the Federal Trade Commission ("FTC"), which is acknowledged as the country's top privacy and security cop.[375] The FTC has wide enforcement in deploying its Section 5 authority to curtail harms in targeted advertising, and the ad industry has the expertise to help the Commission stay current on

[373] *See* Harwell, *supra* note 357; Sherman, *supra* note 359; *cf.* Landon Mion, *Visa Joins Mastercard, AmEx in Specifically Labeling Gun Store Sales*, N.Y. POST (Sept. 11, 2022), https://nypost.com/2022/09/11/visa-joins-mastercard-amex-in-specifically-labeling-gun-store-sales/ [https://perma.cc/SB7R-CVXV].

[374] *See* William McGeveran, *Friending the Privacy Regulators*, 58 ARIZ. L. REV. 959, 971, 980-82 (2016); David Thaw, *Enlightened Regulatory Capture*, 89 WASH. L. REV. 329, 353-62 (2014).

[375] For a similar approach to privacy enforcement, see Roslyn Layton & Simone Celant, How the GDPR Compares to Best Practices for Privacy, Accountability and Trust (Mar. 31, 2017) (unpublished manuscript) https://doi.org/10.2139/ssrn.2944358 [https://perma.cc/GFN6-XBK2] (discussing recommendations from ENISA for implementation of GDPR privacy requirements).

relevant technologies and business practices.[376] The proposed reform seeks to develop working consensus among major advertising interest groups, with input from the FTC, regarding best practices, worst practices, or both for data collection, storage, and transactions.[377]

To gain the benefits of industry expertise and information, the FTC should first convene a working group focused on generating a list of best and worst practices for data collection techniques, storage security, and transactions in personally identifiable information.[378] Participation would be voluntary, though the Commission would encourage firms, trade organizations, and other actors in the advertising ecosystem to take part along with its own experts to ensure that each segment of the industry is represented.[379] Depending upon initial feedback and the complexity of delineating good and bad conduct in each area, the working group might further subdivide itself into issue-specific sections

[376] *See* David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U. L. REV. 287, 296-97 (2014).

[377] *See generally* Bambauer & Teplinsky, *supra* note 340 (discussing regulatory consequences of best and worst software development practices under proposed liability regime); Jim Dempsey, *Standards for Software Liability: Focus on the Product for Liability, Focus on the Process for Safe Harbor*, LAWFARE 1, 2 (Jan. 23, 2024), https://www.lawfaremedia.org/article/standards-for-software-liability-focus-on-the-product-for-liability-focus-on-the-process-for-safe-harbor [https://perma.cc/D88T-QL3W] (discussing floor for software security that would trigger automatic liability and "robust . . . practices" that would confer immunity); Sharona Hoffman & Andy Podgurski, *Securing the HIPAA Security Rule*, 10 J. INTERNET L. 1, 10 (2007) (discussing "best practices" approach to HIPAA Security Rule implementation); Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, 21 RICH. J.L. & TECH. 1, 83 (2015) (discussing "layered" regulatory approach).

[378] *Cf.* THE WHITE HOUSE, NATIONAL CYBERSECURITY STRATEGY IMPLEMENTATION PLAN 30 (2023), https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan_WH.gov_.pdf [https://perma.cc/Z8ML-L9WU] (tasking the "Office of the National Cyber Director, working with stakeholders in academia and civil society, [to] host a legal symposium to explore different approaches to a software liability framework"); *id.* at 38 (directing ONCD, "in conjunction with key stakeholders," to "identify[] and inform[] the development of best practices" to "increase the adoption of secure Internet routing techniques and technology").

[379] *See generally* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 765-66 (2016) (describing working group convened by then-California Attorney General Kamala Harris on privacy policies).

that would make recommendations to the larger gathering.[380] To ensure candor, the working group should keep the substance of discussions in confidence. The identities of participating organizations (and, where a participant is contributing in a personal capacity, their identity) should be made public to build confidence in the collaboration, but neither the substance or valence of a participant's position should be revealed.[381]

The result of these working group consultations would be a set of best and worst practices — likely a combination of principles, standards, and rules — formulated by the FTC, and attributable only to the Commission.[382] The advantage of assigning responsibility to the FTC rather than to working group contributors, either collectively or as a group, is twofold: the FTC is not bound by the group's positions, and participants are free to disavow publicly stances that they took privately if doing so is necessary for business or political reasons. Industry consensus should be treated as a necessary set of best practices, but not automatically as a sufficient one.[383] The final word on adopting recommendations rests with the FTC.

---

[380] *Cf.* Daphné Richemond-Barak, *Can Self-Regulation Work? Lessons from the Private Security and Military Industry*, 35 MICH. J. INT'L L. 773, 784-86 (2014) (describing sub-groups within the International Code of Conduct for Security Service Providers convened by the government of Switzerland).

[381] This requirement, and that of keeping substance confidential, inverts the typical Chatham House Rule that governs such discussions. *See Chatham House Rule*, CHATHAM HOUSE, https://www.chathamhouse.org/about-us/chatham-house-rule (last visited Oct. 5, 2024). Some discussions under the Rule are "off the record," which is closer to this Article's proposal. *Id.*

[382] *See generally* Derek E. Bambauer, *Rules, Standards and Geeks*, 5 BROOKLYN J. CORP., FIN. & COM. L. 49 (2010).

[383] The FTC should be alert to one potential risk: existing industry entities, especially those with significant market share, might advocate for the adoption of more extensive best practices because they would be costly, and thereby hinder smaller competitors and start-ups by imposing regulatory costs. *See* Citron, *supra* note 379, at 802 (noting that "[u]pward regulatory creep could serve as a barrier to entry"). Advertising is a sector with concentrated, sophisticated incumbents who might adopt such a strategy around proposed privacy and security regulation. *See* Steven C. Bennett, *Regulating Online Behavioral Advertising*, 44 J. MARSHALL L. REV. 899, 945-46 (2011); Megan Graham, *Digital Ad Revenue Grew Again in 2022, But Much More Slowly*, WALL ST. J. (Apr. 12, 2023), https://www.wsj.com/articles/digital-ad-revenue-grew-again-in-2022-but-much-more-slowly-41485957 (noting Meta/Facebook, Google, and Amazon earn over 60% of online advertising revenue).

Second, the FTC should seek broader feedback on its draft set of best and worst practices by formally publishing them for notice and comment, engaging in a series of public town hall-style meetings to elicit input, and encouraging commentators from civil society and academia to engage with the recommendations in popular media and scholarly work.[384] Opening the draft for wider review reduces the risk of industry capture of the co-regulatory process.[385] It also ensures consumers and users can evaluate the merits of these tentative legal guidelines since they by definition were not included in the industry working group.[386] After the draft has been sufficiently aired to the public, the FTC should summarize the principal points of feedback from this stage of the process, evaluate the initial recommendations in light of that feedback, make alterations where appropriate, and then explain briefly the Commission's reasons for adopting, or not, the various aspects of public input.[387] After the working group and public feedback stages, the FTC should have a reasonably well-informed understanding of what the advertising industry views as acceptable and unacceptable practices for data collection, storage, and transactions, as well as what the public thinks of those positions.

This Article's proposal leverages both the proverbial carrot and the stick to make use of the public-private guidance described above.[388] The carrot is that compliance with consensus best practices would result in the FTC deploying its regulatory discretion to forgo enforcement for the

[384] *See* Gerard M. Stegmaier & Wendell Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MASON L. REV. 673, 699 (2013).

[385] *See* Wendy E. Wagner, *Administrative Law, Filter Failure, and Information Capture*, 59 DUKE L.J. 1321, 1328 (2010). *But see* Thaw, *supra* note 374, at 370-71 (explaining potential benefits from capture).

[386] In theory, governmental entities such as Congress and the FTC are supposed to represent the public's interest; this is rarely borne out when regulation is produced via interest group negotiations. *See* Jessica D. Litman, *Copyright Legislation and Technological Change*, 68 OR. L. REV. 275, 314 (1989) (noting that the "public, of course, does have a designated representative; acting as that representative is Congress' job description").

[387] If the FTC engages in rulemaking, it will need to follow the relevant statutory mandates for responding to input. *See* 5 U.S.C. § 553 (2018); 15 U.S.C. § 57b-3 (1980).

[388] *See* Vartan Shadarevian, *Broad Optimality in Agency Rulemaking*, 33 STAN. L. & POL'Y REV. 335, 379 (2022).

regulated entity in the three areas covered by the proposal.[389] For example, if an advertising broker followed acknowledged best practices in securing its databases of consumer information, it would not become the target of an FTC investigation or enforcement action even if it suffered a data breach.[390] Security is an imperfect science, and sophisticated attackers such as nation-states are likely to gain access even to well-defended data stores if their personnel devote sufficient resources to the effort.[391] Microsoft is an industry leader in security, yet a hacking group associated with Russia's security services was able to gain access to the mail files of top executives in January 2024.[392]

The stick is that the FTC would commit to treat entities engaged in worst practices as automatically subject to investigation, and those opting out of best practices and suffering a related incident as subject to enhanced scrutiny.[393] Worst practices would become per se unlawful based on the FTC's Section 5 authority; it has effectively so held before

[389] The FTC has, at least in theory, already committed to a similar approach to telecommunications security regulation. *See* Scott Shackelford, Andrew A. Proia, Brenton Martell & Amanda Craig, *Toward a Global Cybersecurity Standard of Care? Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 303, 306 (2015).

[390] *See* Bambauer & Teplinsky, *supra* note 340, at 2 (describing safe harbor structure for software that provides "immunity for following defined best practices, and clear liability for engaging in terrible ones").

[391] *See* Bambauer, *Ghost in the Network*, *supra* note 354, at 1015 (describing successful cyberattack by the United States on Iran's nuclear enrichment program despite sophisticated defenses such as network air gaps); Derek E. Bambauer & Oliver Day, *The Hacker's Aegis*, 60 EMORY L.J. 1051, 1062 (2011) (noting rising incidence of zero-day vulnerabilities).

[392] *See* Jordan Novet & Rohan Goswami, *Microsoft Executive Emails Hacked by Russian Intelligence Group, Company Says*, CNBC (Jan. 19, 2024, 4:49 PM), https://www.cnbc.com/2024/01/19/microsoft-executive-emails-hacked-by-russian-intelligence-group-company-says.html [https://perma.cc/NMS5-BZ4J].

[393] *See* William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1193-95 (2019) (describing security "worst practices"). The requirement that a security incident be related to the subject areas of the proposal leaves the FTC with discretion to pursue advertisers who are compliant in data collection, storage, and transactions, but who engage in misconduct in other areas, such as violating constraints on advertising to children. *See* Children's Online Privacy Protection Rule, 78 FED. REG. 3972, 3972 (Jan. 17, 2013) (updating 16 C.F.R. 312).

for certain privacy- and security-related conduct or omissions.[394] The co-regulatory model enables the FTC to draw upon distributed information that is largely held by private entities to generate a zone of strict liability, a zone of immunity, and information to inform negligence-style analysis between the prior two types of conduct for data collection, storage, and transactions.[395] The co-regulatory model is usefully flexible — it offers firms some leeway in managing data collection, data storage, and transactions in personal information so long as they avoid clearly unacceptable conduct (worst practices), engage in plainly reasonable behavior (best practices), or both.

One advantage of this reform proposal is that there are several different ways that it could be implemented. Ideally, Congress would pass, and the President would sign, enabling legislation that authorizes the FTC to convene the working group, to gather feedback on its recommendations, and to deploy them in its enforcement work. Should pessimism about near-term Congressional action prove well-founded, though, there are other paths to utilizing the new guidelines. The FTC could pursue rulemaking under its statutory authority.[396] That path is made harder by the more elaborate procedures the Commission must follow in its consumer protection rulemaking relative to other administrative agencies.[397] The last option is the easiest for the

[394] *See, e.g.*, LABMD, Inc. v. FTC, 894 F.3d 1221, 1224 (11th Cir. 2018) (allowing employee to install peer-to-peer software on computer with access to sensitive data) (injunction reversed on appeal); FTC v. Wyndham Worldwide Corp., LLC, 799 F.3d 236, 240-42 (3d. Cir. 2015) (storing payment card information in clear text, failing to segment networks, and failing to change default passwords on systems); Complaint, *In re* EPN, Inc., No. C-4370 (F.T.C. Oct. 3, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/10/121026epncmpt.pdf (allowing employee to install peer-to-peer software on computer with access to sensitive data).

[395] *See* Derek E. Bambauer, *Cybersecurity for Idiots*, 106 MINN. L. REV. HEADNOTES 172, 175-76 (2021) [hereinafter Bambauer, *Cybersecurity for Idiots*]; Amanda N. Craig, Scott J. Shackelford & Janine S. Hiller, *Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis*, 52 AM. BUS. L.J. 721, 721-23 (2015).

[396] *See* Justin (Gus) Hurwitz, Chevron *and the Limits of Administrative Antitrust*, 76 U. PITT. L. REV. 209, 232-37 (2014) (tracing evolution of FTC's Section 5 rulemaking powers).

[397] *See id.* at 235-37 (describing shift from "substantive rulemaking authority . . . governed by the standard Administrative Procedure Act ('APA') notice-and-comment

Commission, although perhaps it is also the most controversial. The FTC generates a considerable body of soft law from the investigations it decides to undertake, the settlements into which it enters, the guidance documents it creates, and the public statements of the commissioners and other senior officials.[398] Entities regulated by the FTC wisely place considerable emphasis on this soft law as informal yet accurate guidance as to how the Commission will wield its enforcement discretion.[399]

The FTC already has considerable expertise in privacy and security matters and should use that knowledge to generate initial ideas for discussion with industry. It would be particularly helpful if the Commission concentrated on easy regulatory cases during the initial phase of consultations to build trust and create the potential for quick returns once the guidelines are implemented.[400] This sort of borrowing, or "regulatory diffusion," has a number of potential benefits, including the ability to learn from the experience of other regulators ("leapfrogging") and to conserve resources in crafting rules.[401] For example, with transactions in personally identifiable information, it seems plausible that a "know your customer" requirement could designate a set of procedures for determining whether a particular potential transferee of data is sufficiently reputable and reliable to predict that the risk of misuse is low.[402] Here, too, there could be designation of known reliable entities and known bad actors — another best practices and worst practices example.[403] In addition, the

rulemaking procedures" to rulemaking with "additional procedural requirements" via legislation in 1980 and 1994).

[398] *See* Solove & Hartzog, *supra* note 215. *But see* Hurwitz, *supra* note 215 (criticizing these informal practices).

[399] *See* sources cited *supra* note 398.

[400] *See* Bambauer, *Cybersecurity for Idiots*, *supra* note 395, at 172-76 (describing cybersecurity vulnerabilities that can be readily remediated as fruitful regulatory targets).

[401] *See* Jennifer Nou & Julian Nyarko, *Regulatory Diffusion*, 74 STAN. L. REV. 897, 939 (2022).

[402] *See* Christina Parajon Skinner, *Coins, Cross-Border Payments, and Anti-Money Laundering Law*, 60 HARV. J. ON LEGIS. 285, 307-11, 323-26 (2023).

[403] For one example of a list of prohibited actors, see the list of Specially Designated Nationals and Blocked Persons maintained by the Office of Foreign Assets Control ("OFAC") within the U.S. Department of the Treasury. *Specially Designated Nationals Lists*, OFF. FOR. ASSETS CONTROL (last updated Feb 2, 2024),

collaboration could develop a set of preferred contractual provisions (for example, including a prohibition on transfer to entities listed as known bad actors, as described previously) and indeed model contracts for data transactions.[404]

For data collection techniques, the FTC might initially propose a set of baseline security precautions about the code or mechanisms used to gather data (to reduce the risk of malvertising and malware)[405] and perhaps some standards for data gathering limitations or minimization.[406] And for data storage, items might involve security measures and testing,[407] along with perhaps data-specific constraints such as temporal restrictions or data expiration.[408] These items are neither required nor certain components of the output from the collaborative process. Rather, they are examples of issues where consensus may be possible and where the FTC may be able to draw upon its privacy and security work to suggest relatively easy starting points for discussion.

This Article's co-regulatory proposal has two important limitations, both subject to change based upon data from this quasi-experiment. The first is that its enacting legislation would sunset after five years.[409] This

https://ofac.treasury.gov/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists [https://perma.cc/EH44-5BZE]. *See generally* John R. Liebman & Kevin J. Lombardo, *A Guide to Export Controls for the Non-Specialist*, 28 LOY. L.A. INT'L & COMP. L. REV. 497 (2006).

[404] *See* Paul M. Schwartz, *Information Privacy in the Cloud*, 161 U. PA. L. REV. 1623, 1659 (2013).

[405] *See* Rita M. Cain, *A Study of Spyware Enforcement Actions in Pursuit of Sound Internet Advertising Policy*, 5 J.L. & POL'Y INFO. SOC'Y 291, 298-309 (2009).

[406] *See* Rebecca Balebako, Cristian Bravo-Lillo & Lorrie Faith Cranor, *Is Notice Enough: Mitigating the Risks of Smartphone Data Sharing*, 11 J.L. & POL'Y INFO. SOC'Y 279, 284, 298-99, 306, 312-14 (2015).

[407] *See* McGeveran, *supra* note 393, at 1155-56.

[408] *See* Ira S. Rubinstein & Nathaniel Good, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*, 28 BERKELEY TECH. L.J. 1333, 1379-82 (2013).

[409] The FTC could commit to a five-year sunset if it adopted the proposal through rulemaking or soft law. Sunset provisions can allow legislators or regulators to evaluate the success of a particular intervention and, in some cases, to build political support for it. *See* Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753, 1800 (2019) (proposing an "amendment to Section 230 [that] could include a sunset provision paired with data-gathering requirements that would empower Congress to make an informed decision on

sunset provision would push the Commission and industry alike to study and monitor the effects of this intervention on the advertising marketplace.[410] It would force advocates for continuing the intervention to make their case to a different Congress based on the program's record.[411]

The second limitation is that the reform would not affect other regulators such as state attorneys general or private plaintiffs. If sufficient information were available, it would be desirable to have a uniform enforcement landscape such that compliance with best practices would insulate an advertising entity from relevant liability from any source.[412] Realistically, though, the FTC might have inaccurate or insufficient information, or might simply get things wrong.[413] Enforcement by other actors could have the salutary effects of surfacing additional information or offering alternative interpretations of existing data.[414] Allowing other regulators to continue to operate independently

renewal"); Craig Konnoth, *Health Data Federalism*, 101 B.U. L. REV. 2169, 2188 (2021) (describing Iowa's health data commission, which was initially subject to sunset, but made permanent after six years). For example, the USA PATRIOT Act of 2001 contained a number of sunset provisions. *See* U.S. DEP'T OF JUST., USA PATRIOT ACT: SUNSETS REPORT (2005), https://www.justice.gov/archive/olp/pdf/sunsets_report_final.pdf [https://perma.cc/56JS-EY2H] (reporting on results and criticism of various provisions with sunset dates but recommending extension of all such provisions).

[410] For an analogous approach to measuring effectiveness of an intervention, see MATTHEW H. FLEMING & ERIC GOLDSTEIN, HOMELAND SEC. STUD. & ANALYSIS INST., METRICS FOR MEASURING THE EFFICACY OF CRITICAL-INFRASTRUCTURE-CENTRIC CYBERSECURITY INFORMATION SHARING EFFORTS 4, 33 (2012).

[411] Congress could remove the sunset provision before the legislation expired, of course, and has done so in other areas. *See* Derek E. Bambauer, *Everything You Want: The Paradox of Customized Intellectual Property Regimes*, 39 BERKELEY TECH. L.J. 101, 142-43 (2024) (describing Congressional removal of sunset provision from Vessel Hull Design Protection Act of 1998 after boating industry lobbying).

[412] There are advertising regulations with similar pre-emption features such that compliance with federal law ensures immunity. For example, the CAN-SPAM Act of 2003 pre-empts any conflicting state anti-spam laws except for those that prohibit falsity or deception. 15 U.S.C. § 7707(b)(1).

[413] *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 273-75 (2011).

[414] *See, e.g.*, Charles M. Davidson & Michael J. Santorelli, *Federalism in Transition: Recalibrating the Federal-State Regulatory Balance for the All-IP Era*, 29 BERKELEY TECH. L.J. 1131 (2014).

is particularly worthwhile in the early phases of this Article's proposed reform, when the advertising industry and FTC are performing the hard work of sharing information and attempting to generate consensus. Preemption could be more helpful once the process plays out and the working group's proposals have been more thoroughly reviewed.

If the co-regulatory model works well enough, Congress should consider extending it beyond the five-year sunset period. Legislation to that end should consider two additional features. First, it should require reporting on the effects of this co-regulatory model at designated intervals, such as every five years, so that Congress could revisit the desirability of this intervention.[415] Second, the legislation should pre-empt, or block, suits by state attorneys general or private plaintiffs based on conduct covered by the co-regulatory regime if the FTC has issued an advisory opinion that the challenged activities were not harmful on net.[416] This would allow the Commission to take the lead in advertising regulation while also enabling it to delegate enforcement if it desired to do so.

This co-regulatory model[417] (or, to use the term Americans tend to prefer, "public-private partnership")[418] has several other potential benefits. One is that it could enable regulators such as the FTC to

[415] *See supra* note 409.

[416] The legislation could also authorize plaintiffs or attorneys general to seek confirmation from the FTC that it does not plan to issue such an opinion — a sort of regulatory "no action" letter. *Cf.* Ryan Snyder, *Trading Nonenforcement*, 39 GA. ST. U. L. REV. 777, 795-96 (2023) (describing informal U.S. Securities and Exchange Commission commitments not to engage in enforcement after issuing a no-action letter regarding the transaction). Preemption of conflicting enforcement, and enforcers, based on federal policy judgments is not uncommon in technology regulation. *See* 17 U.S.C. § 301 (preempting "all legal or equitable rights that are equivalent to any of the exclusive rights within the general scope of [federal] copyright"); 47 U.S.C. § 230(e)(3) (barring enforcement of state civil and criminal codes inconsistent with this section of federal law, which provides broad immunity to interactive computer services and their users); Jessica D. Litman, *Copyright Compromise and Legislative History*, 72 CORNELL L. REV. 857, 873 (1987) (describing industry-specific provisions of Copyright Act drafted through industry group negotiations under auspices of the Register of Copyrights); *supra* note 412 (commercial e-mail advertising).

[417] *See* McGeveran, *supra* note 374, at 980-82; Thaw, *supra* note 374, at 353-62.

[418] *See* Margot E. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. CAL. L. REV. 1529, 1560-64 (2019).

conserve resources if private organizations are capable of and willing to undertake some enforcement work. For example, the National Advertising Division might handle adjudication of at least some allegations of violations of the best or worst practices consensus.[419] In the late 1960s and early 1970s, the advertising industry faced increasing calls for regulation of its activities, along with heightened scrutiny by existing governmental regulators. In an attempt to head off greater oversight, a set of industry interest groups (including the Council of Better Business Bureaus) established a voluntary self-regulatory organization, the National Advertising Division ("NAD").[420] The NAD addresses concerns and referees disputes over the accuracy of national advertising both through its own monitoring efforts and through referrals (effectively, complaints) from consumers and competitors, although the last route constitutes the large majority of its activity.[421] The NAD requires that complaints be substantiated in order to be pursued, and has discretion whether to pursue referrals.[422] Investigations are handled by the NAD's staff attorneys, who have considerable experience and expertise with handling advertising matters.[423] Participation in the NAD dispute resolution process is voluntary; however, if the NAD closes an investigation due to a defendant's refusal to participate, it notifies the FTC, and it is common knowledge that such matters "go to the top of the FTC's pile."[424] At the conclusion of an investigation, the NAD issues a written decision concluding either that the advertising at issue should be changed or that it deems the ad sufficiently substantiated.[425] The NAD maintains a database of its opinions, and the risk of negative publicity from an adverse decision gives the Division's enforcement power its efficacy,

[419] *See* Terri Seligman & Hannah Taylor, *Navigating the National Advertising Division*, ABA LANDSLIDE, https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2018-19/march-april/navigating-national-advertising-division/ (last visited Oct. 5, 2024) [https://perma.cc/TV3Z-4KCJ].

[420] This is a slight simplification of the organizational complexities of the organization's formation. For a longer account, see Seligman & Taylor, *supra* note 419.

[421] *Id.*

[422] *Id.*

[423] *Id.*

[424] *Id.*

[425] *Id.*

particularly since trade publications like *Ad Age* (previously *Advertising Age*) and national media outlets often report on NAD decisions.[426] In addition, NAD decisions are sometimes accorded some evidentiary weight by federal courts during litigation.[427]

Given the Division's record and expertise, the Commission might use the NAD as a quasi-trial court or clearinghouse by encouraging industry entities and even consumers to file complaints with the Division first rather than seeking an FTC investigation.[428] The NAD's dispute resolution system is voluntary, but has the advantages of sophisticated staff, considerable informal power to jawbone violators, and a record of written decisions that can guide behavior by other entities.[429] In addition, the FTC has a track record of supporting the NAD's role in industry self-regulation; moreover, when both entities investigate a matter, the FTC's decisions have largely tracked those of the NAD.[430] In turn, the NAD typically follows FTC guidance on advertising issues.[431]

Under the co-regulatory model, the NAD and the FTC could collaborate by employing the same standards to adjudicate alleged misconduct.[432] If an NAD investigation found that the respondent or defendant did not breach the consensus guidelines, the FTC could agree to respect that decision and forgo its own investigation, except in cases where the NAD's finding was clearly erroneous.[433] Similarly, the FTC could treat an NAD finding that the respondent or defendant had

[426] *See* Arthur Best, *Controlling False Advertising: A Comparative Study of Public Regulation, Industry Self-Policing, and Private Litigation*, 20 GA. L. REV. 1, 14 (1985).

[427] *See, e.g.*, Russian Standard Vodka (USA), Inc. v. Allied Domecq Spirits & Wine USA, Inc., 523 F. Supp. 2d 376, 384-85 (S.D.N.Y. 2007) (granting 30-day stay in litigation to allow time for NAD to issue decision on dispute between parties because organization was a "highly reputable institution . . . [whose] expert view . . . would be extremely useful in resolving remaining claims in the complaint," and because the NAD decision would likely promote settlement, thereby conserving public resources).

[428] *See* Best, *supra* note 426, at 14.

[429] *See id.*; *see also* Seligman & Taylor, *supra* note 419.

[430] *See* John E. Villafranco & Katherine E. Riley, *So You Want to Self-Regulate? The National Advertising Division as Standard Bearer*, 27 ANTITRUST 79, 79-80 (2013).

[431] *Id.* at 80.

[432] *See id.*

[433] *See id.* at 80-81. This deference would be a change for the FTC, which performs its own analysis of matters referred to it by the NAD, at least formally. *See id.* at 80.

violated the guidelines, but refused to change its conduct, as automatic grounds for launching its own enforcement action — again, unless the NAD's outcome was in clear error.[434] This collaborative adjudication approach would offload some enforcement of the co-regulatory model to a private, expert body whose decisions are typically accepted by advertising industry entities, with the backstop of FTC action for circumstances where the NAD plainly made a mistake or where an entity found to have violated the agreement refused to change course.

Another potential benefit from the co-regulatory model is increased regulatory certainty, which could encourage innovation that is made risky due to a complex, shifting legal landscape.[435] Regulatory uncertainty is one factor that undercuts innovation.[436] With advertising, the risk to innovation is demonstrated by the impact of Google's targeted advertising ban for children's games.[437] Patches and new features dropped by 17% for games where such advertising was banned relative to unaffected ones.[438] The effects scaled — the more dependent a game was upon advertising for revenues, the greater the drop in innovation as measured by new features and fixes.[439] Even if innovation did not change in absolute terms, the change in Google's private regulatory approach shifted where it occurred: developers invested less in children's games and more in ones eligible for targeted advertising.[440] Developers and firms could deploy targeted ads with fewer worries about legal liability based on the guidance available from the proposed co-regulatory model.

Overall, this Article's proposed co-regulatory model would combine industry expertise with FTC enforcement, generating a set of best and

---

[434] The FTC should also increase its transparency about how it treats referrals from NAD. From 2001 to 2013, the Commission "made public the results of only five of the twenty-one cases referred to it for refusal to participate in the NAD process." *Id.* at 81.

[435] *See* Sofia Ranchordás, *Innovation Experimentalism in the Age of the Sharing Economy*, 19 LEWIS & CLARK L. REV. 871, 917-24 (2015) (discussing temporary regulations and sunrise clauses as mechanisms to spur innovation by increasing legal predictability).

[436] *See* Tal Z. Zarsky, *The Privacy-Innovation Conundrum*, 19 LEWIS & CLARK L. REV. 115, 139 (2015) (observing "[r]egulation is noted for . . . causing uncertainty and delay").

[437] Kircher & Foerderer, *supra* note 94, at 1071-72.

[438] *Id.*

[439] *Id.*

[440] *Id.*

worst practices for data transactions, collection techniques, and storage. Entities that implemented best practices, and avoided worst ones, would be safe from FTC enforcement actions related to those choices. Those that engaged in worst practices, by contrast, would be automatically targeted for investigation.

CONCLUSION

Targeted advertising presents a major challenge for U.S. regulators. The practice is more lucrative than its untargeted counterpart, and many popular Internet applications depend heavily, if not exclusively on revenues from it. Simultaneously, targeted advertising creates important privacy risks that are troubling to the consumers who use those applications. Consumers are increasingly discontent, which explains why targeted advertising has vaulted to the top of the policy agenda at both state and federal levels in the United States in recent years. Those same users, though, will not welcome interventions that damage or destroy online services, such as Facebook, that are both extraordinarily popular and highly dependent on targeted advertising. Reform that is both effective and politically palatable must find a path between these two pitfalls. This Article proposes such a measure: a co-regulatory model that draws upon expertise and generates political supports from all participants in the debate, meshing the power of FTC oversight with the insights of industry expertise.

This proposed intervention is likely to become even more necessary in the coming years, as targeted advertising moves beyond purely commercial transactions and becomes enmeshed in deeply contentious political and social conflicts. Consider abortion and climate change. First, pregnancy resource centers, which oppose abortion services and seek to convince women not to obtain abortions, have employed location-aware technologies — geofencing — to send ads to women who are visiting or are in the vicinity of abortion service providers.[441] One

[441] *See* Nicole Hunt, *Pregnancy Resource Centers Condemned for the Use of Targeted Advertisements to Reach Abortion-Minded Women*, PREGNANCY HELP NEWS (June 7, 2023), https://pregnancyhelpnews.com/pregnancy-resource-centers-condemned-for-the-use-of-targeted-advertisements-to-reach-abortion-minded-women [https://perma.cc/X7X9-GLW6]; Byron Tau & Patience Haggin, *Antiabortion Group Used Cellphone Data to Target Ads to Planned Parenthood Visitors*, WALL ST. J. (May 18, 2023), https://www.wsj.com/

Wisconsin group used geofencing techniques to identify the phones brought into the offices of health care providers such as Planned Parenthood and then used the device IDs to target ads to their owners on social media platforms such as Facebook and Snapchat.[442] Similar campaigns ran in New Jersey, California, Florida, and Colorado.[443] Abortion rights groups expressed concerns that just the use of targeted advertising in this context is problematic from a health privacy perspective.[444] And while advertising can often lead to outcomes that are beneficial for all involved, such as when a consumer purchases a product that they did not previously know about but ultimately find useful, the abortion geofencing campaign is likely one that is a zero-sum game. Abortion opponents want to persuade women seeking an abortion to forgo a course of action that they view as morally unacceptable. Abortion advocates want to enable women to make that choice without personally targeted pressures that come at a vulnerable moment and may have a chilling effect because of their use of personal data. Targeted advertising reform must grapple candidly with that debate, because its content will affect not just ads, but abortion.

Second, researchers used targeted advertising to display ads about the risks of climate change to members of the Republican Party in a pair of competitive Congressional districts: Missouri's second district and Georgia's seventh district.[445] The video ads were served to Facebook and YouTube users in those districts identified, through the use of personal

articles/antiabortion-group-used-cellphone-data-to-target-ads-to-planned-parenthood-visitors-446c1212. The FTC, under the Biden administration, has begun to address this issue. *See* FTC, *FTC v. Kochava, Inc.*, https://www.ftc.gov/legal-library/browse/cases-proceedings/ftc-v-kochava-inc (last updated July 15, 2024) [https://perma.cc/8BHD-DGNA]; Cristiano Lima-Strong, *FTC Extends Data Broker Crackdown as Khan's Term Nears Likely End*, WASH. POST (Dec. 3, 2024), https://www.washingtonpost.com/politics/2024/12/03/ftc-extends-data-broker-crackdown-khans-term-nears-likely-end/.

442 *See* sources cited *supra* note 441.

443 *See* sources cited *supra* note 441.

444 *See* Nik Popli & Vera Bergengruen, *Lawmakers Scramble to Reform Digital Privacy After* Roe *Reversal*, TIME (July 1, 2022), https://time.com/6193224/abortion-privacy-data-reform/ [https://perma.cc/8FQX-7B5H].

445 Matthew H. Goldberg, Abel Gustafson, Seth A. Rosenthal & Anthony Leiserowitz, *Shifting Republican Views on Climate Change Through Targeted Advertising*, 11 NATURE CLIMATE CHANGE 573, 573-77 (2021).

data, as politically conservative.[446] The advertising campaign generated significant effects on those who viewed on questions such as whether global warming was occurring, whether they found it personally important, and whether global warming would have moderate to great effects on future generations.[447] Statistical analysis showed that the ads had no effect on people enrolled as Democrats or Independents, but significant effects on Republicans and on those who did not affiliate with a political party.[448] As with other targeted advertising, the researchers conclude that the major effects are derived from the greater exposure of Republicans in these areas to the content rather than to any particularly greater persuasive effect on Republicans.[449] The study shows that targeted advertising can have significant effects on highly controversial, non-pecuniary topics about which there are significant partisan political splits.[450]

Abortion and climate change are not the only hot-button issues that have become entwined with regulatory questions about targeted advertising; firearms[451] and cannabis are becoming so as well. Regulation of targeted advertising will only become more difficult as time passes and as commercial and political content intermingle in the ad creative.

---

[446] *Id.* (describing use of advertising software from Centro).

[447] *Id.*

[448] *Id.*

[449] *Id.*

[450] *See* David Sherfinski, *U.S. Climate Ads by Conservatives, for Conservatives, Shift Views*, REUTERS (June 30, 2021), https://www.reuters.com/article/us-usa-climate-change-advertising-trfn/u-s-climate-ads-by-conservatives-for-conservatives-shift-views-idUSKCN2E61HM/. Climate change is a highly polarized issue: among Democrats, 78% view climate change as a major threat to the U.S.; among Republicans, 23% do. *See* Alec Tyson, Cary Funk & Brian Kennedy, *What the Data Says About Americans' Views of Climate Change*, PEW RSCH. CTR. (Aug. 9, 2023), https://www.pewresearch.org/short-reads/2023/08/09/what-the-data-says-about-americans-views-of-climate-change/ [https://perma.cc/4APT-US9W] (noting "perceptions are tied more strongly to people's beliefs about climate change — and their partisan affiliation — than to local conditions").

[451] *See* Katie Deighton, *Twitter Bolsters Charm Offensive with Cannabis Advertisers*, WALL ST. J. (Apr. 26, 2023), https://www.wsj.com/articles/twitter-bolsters-charm-offensive-with-cannabis-advertisers-2b2c1599; John O'Connor, *Illinois to Ban Advertising for Guns Allegedly Marketed to Kids and Militants*, AP (Aug. 7, 2023), https://apnews.com/article/illinois-gun-advertising-legislation-minors-militants-3d72ed4b2febbf9e462bd854a40faa0c.

This Article's co-regulatory model can meaningfully address privacy harms, reduce political opposition to reform, and evolve based on continuing analysis of empirical data to ensure that its intervention aims accurately at targeted advertising's problems without injuring its benefits.