Institute for New Economic Thinking

Working Papers
ineteconomics.org/workingpapers

AI, Antitrust & Privacy

Maurice E. Stucke†

Working Paper No. 236

June 25th, 2025

ABSTRACT

Generative artificial intelligence (AI) is reshaping how companies profile individuals, create and target ads, and influence behavior—often in ways that undermine privacy, autonomy, and democracy. This article explores a critical but overlooked question: how AI affects the relationship between competition and privacy. Increased competition in the AI supply chain may seem like a solution to Big Tech's dominance, but when firms are rewarded for surveillance and manipulation, more competition can actually make things worse.

Drawing on recent market trends and twenty state privacy laws, the Article shows how the existing legal frameworks—even those designed to protect privacy—fall short and may unintentionally entrench the power of few data-opolies. It argues that privacy and competition must be addressed together, not in silos, and offers specific legislative reforms to help align business incentives with public interests. Without stronger guardrails, AI risks accelerating a race to the bottom—fueled not only by powerful technologies, but by well-intentioned, but flawed policies.

https://doi.org/10.36687/inetwp236

JEL codes: K21, K24, L40, L41, L50, O33

Keywords: Antitrust, privacy, monopolies, data, artificial intelligence

† Douglas A. Blaze Distinguished Professor of Law, University of Tennessee Winston College of Law.

INTRODUCTION

How will generative artificial intelligence (hereinafter AI) likely impact your life in 2040?[1] When asked this question in 2023, most Americans and AI experts were negative on many parameters (with the AI experts especially negative):

- 79% of the AI experts expected AI to harm personal privacy (which was higher than the two-thirds of polled Americans who expressed that);
- 54% of AI experts expected AI to harm basic human rights (versus 41% of the polled Americans);
- 67% of AI experts expected AI to harm politics and elections (versus 51% of the polled Americans); and
- 52% of AI experts expected AI to worsen the level of civility in society (versus 40% of the polled Americans).[2]

Notably absent from that survey was AI's impact on competition.

In parallel with the debate over AI's broader effects, antitrust scholars and enforcers are debating how the emerging AI foundation model supply chain may evolve and whether the technology may entrench the market power of a few firms. Competition authorities are concerned about the increasing concentration in this emerging supply chain. In particular, the digital economy has several factors and characteristics that can lead to concentrated markets. Are there similar factors in the emerging AI foundation model supply chain that will lead to "winner-take-most-or-all"? Could AI herald new business models and innovations that disrupt the dominant ecosystems of Google, Apple, Meta, Amazon, and Microsoft (GAMAM or data-opolies for short)? Or will these ecosystems also dominate key segments of the AI foundation model supply chain? Competition authorities naturally seek to promote competition in this supply chain.

---

[1] As used herein, generative artificial intelligence means machine learning models that

> *leverage deep neural networks to emulate human intelligence (i.e. by imitating information processing of neurons in the human brain) by being exposed to data (training) and finding patterns that are then used to process previously unseen data. This allows the model to generalise based on probabilistic inference (i.e., informed guesses) rather than causal understanding. Unlike humans, who learn from only a few examples, deep neural networks need hundreds of thousands, millions, or even billions, meaning that machine learning requires vast quantities of data.*

OECD, AI, Data Governance & Privacy: Synergies and Areas of International Co-Operation, OECD Artificial Intelligence Papers No. 22, at 18 (June 2024), https://www.oecd.org/en/publications/ai-data-governance-and-privacy_2476b1a4-en.html.

[2] Elon University, The Impact of Artificial Intelligence by 2040: National public opinion poll findings (Feb. 2024), https://imaginingthedigitalfuture.org/wp-content/uploads/2024/02/AI2040-Report-public-opinion-poll-white-paper-1.pdf; Lee Rainie & Janna Anderson, A New Age of Enlightenment? A New Threat to Humanity?, Elon University (Feb. 2024), https://imaginingthedigitalfuture.org/wp-content/uploads/2024/02/AI2040-FINAL-White-Paper-2-2.29.24.pdf.

The two ongoing debates over AI (increased competition and protecting privacy) are largely siloed from each other. Competition officials focus on AI's impact on competition without considering AI's broader implications (which they deem beyond antitrust's scope). Those debating AI's wider implications for privacy, human rights, elections, and civility are not considering the role of competition. Missing from both debates is how exactly will AI affect the relationship between competition and privacy. Specifically, how will AI impact profiling and behavioral advertising? Will more competition in the AI supply chain improve (or harm) privacy, autonomy, and well-being? What are the broader implications on democracy, social discourse, and civility when competition among the foundation models increases? Understanding this relationship between competition and privacy is important for several reasons.

First, neither privacy nor competition concerns can be addressed independently; privacy and competition policies must work in tandem. The conundrum is this: In many digital markets where the product or service is ostensibly free (think video streaming, Internet search engines, maps, social networks), privacy can be a critical non-price parameter of competition. However, many digital firms often fail to provide the privacy protections that individuals desire. If the market failure is due to a lack of meaningful competition, such as a dominant firm exercising its market power by eroding privacy protections, then in that case, current or more advanced antitrust tools may address the problem. However, if the market failure is due to misaligned incentives (i.e., where firms collect personal data *about* us but not *for our* benefit), then more competition will not fix the issue. Instead, injecting more competition in the AI supply chain can worsen privacy, autonomy, well-being, and democracy.

Second, competition can often enhance privacy when the incentives of market participants align with those of individuals. This alignment, however, does not arise organically. Instead, policymakers must rely on legal guardrails (here, privacy measures) to ensure that competition is a race to the top rather than the bottom. Once these guardrails are in place, competition and privacy will often, but not always, be complementary, where firms compete to promote individuals' privacy.

Third, in crafting these guardrails, privacy and competition officials, as well as courts, must assess the impact of privacy rights on curbing toxic competition while promoting healthy competition. As this Article explores, eighteen states, ostensibly seeking to promote privacy by giving their residents certain opt-out rights, are actually helping data-opolies maintain their dominance. This is not their intent, as the states are simultaneously suing these data-opolies for, among other things, degrading the privacy of their residents.

This Article is the first to explore how AI will likely affect the relationship between competition and privacy regulation in the context of behavioral advertising and profiling. While policymakers were concerned about attention manipulation and behavioral advertising before the emergence of the AI foundation models ChatGPT, Llama, and Gemini, Part I explores how this AI will hasten

the race to the bottom and increase tensions between competition and privacy regulation. Individuals found it challenging to avoid profiling, manipulation and behavioral advertising before the advent of AI. It will become even harder when AI deciphers our emotions and learns better ways to manipulate us. While antitrust authorities will seek to promote competition along the AI supply chain, that increased competition, given the current misaligned incentives, will likely further degrade privacy, human autonomy, and well-being.

In the case of misaligned incentives, increased competition (and antitrust policies generally) will not offer respite. As a 2024 ICN Report noted, in these situations, jurisdictions can use "consumer protection and privacy measures to align incentives and help ensure that the competition is a race to the top rather than the bottom."[3] Since the United States lacks a comprehensive federal privacy framework, Part II turns to 20 recently enacted state privacy laws to see whether they can provide sufficient guardrails to reorient the current toxic competition to a race to the top. These privacy laws incorporate many Fair Information Practice Principles, such as providing their residents the right to access their personal data, and correct or delete the information.[4] Most state laws also incorporate data minimization principles, such as limiting the types of personal information firms can collect, its use internally within the organizations, and for how long the firms can keep the data.[5] As Part II explores, eighteen of these 20 states, including the three most populous states (California, Texas, and Florida), enable (or will soon allow) their residents to opt out of profiling and targeted advertising.

The bad news, as Part III examines, is that while these states afford their residents greater privacy protections regarding behavioral advertising and profiling, their laws all share several significant shortcomings that paradoxically will empower the data-opolies and hinder our privacy, autonomy, democracy, and well-being.

Part IV proposes several legislative amendments to these state privacy laws to improve both privacy and competition and curb the likely harms from AI-driven behavioral advertising and profiling.

---

[3] International Competition Network, Competition law enforcement at the intersection between competition and privacy: Agency considerations, at 13 (2024), https://www.internationalcompetitionnetwork.org/wp-content/uploads/2024/12/Intersection-project-agency-considerations.pdf [hereinafter ICN Report].

[4] For more on the FIPPs, see http://www.oecdprivacy.org. For an overview of the state privacy laws' FIPPs, see, IAPP, US State Privacy Legislation Tracker 2025, https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf.

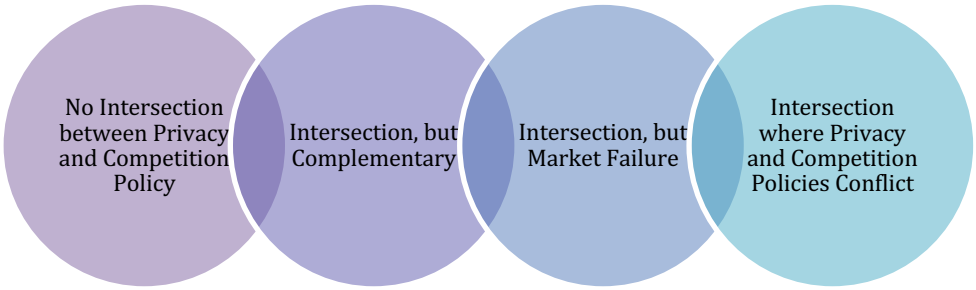
[5] See IAPP, *supra* note.

I. How AI Will Likely Increase the Potential Tensions Between Competition And Privacy Regulation

A. Relationship Between Privacy and Competition Policy

In 2024, the International Competition Network published its report, *Competition Law Enforcement at the Intersection between Competition and Privacy: Agency Considerations*, addressing two issues of increasing importance in the digital economy: first, what is the relationship between privacy and competition policy? Second, when privacy and competition concerns intersect, what factors should competition agencies assess in their decision-making process? The report was the result of significant work by its member competition agencies, including the U.S. Federal Trade Commission (FTC), in gathering feedback from over 100 competition and privacy officials worldwide.

In cataloging the relationship between privacy and competition policy, the report advanced the debate on when these policies can conflict, outlining the following four categories[6]:



Under the first category, privacy and competition policies do not intersect. Many competition cases do not raise privacy issues (such as a typical cartel where competitors agree to rig bids or fix prices). Likewise, many privacy claims do not raise competition concerns, such as landlords who spy on their tenants.[7]

In the second category, privacy and competition policies intersect but are complementary. Here, privacy is an important non-price parameter of competition. When competition increases, privacy can improve. This second category includes exploitative abuses of dominance, where the extraction of too much personal data is like charging an excessive price.[8]

---

[6] ICN Report, *supra* note, at 4.

[7] *Id*. at 5.

[8] *Id*. at 5-11.

The third category is of interest for our purposes – where privacy and competition policies intersect, but there is a market failure. As the ICN Report notes:

> *. . . even when beyond the competition agency's purview, it is important for the agency to recognize that promoting transparency of the companies' privacy practices, lowering entry barriers, making the markets more contestable, and increasing the number of rivals will not necessarily improve privacy protection, when the market participants' incentives are not aligned with the consumers' interests. Competition will increase, but not privacy. When the incentives are misaligned, firms will collect and use personal data about individuals, but not necessarily for their benefit.*[9]

Here, as competition agencies recognize, competition, at times, is not a panacea, and when toxic, it can make things worse. Toxic competition can arise under several scenarios, one of which is when incentives are misaligned.[10] One example of misaligned incentives in the digital economy is behavioral advertising. Unlike contextual advertising, which targets audience members broadly based on the context of the publication's topics or audience demographics (such as fitness ads in running magazines), behavioral advertising targets "advertising and promotions to individuals based inter alia on the personal data collected about the person's online and offline activities."[11] As FTC Commissioner Rohit Chopra discussed in one of the agency's cases against Google:

> *Behavioral advertising, unlike contextual advertising, is about targeting each individual – a demographic of one. Google is able to do this by tracking and collecting an enormous amount of information on users' behavior wherever Google embeds its technology. This includes activity on their phones, home devices, on YouTube, and nearly everything they do online. When individuals use a mobile device with Google's Android operating system or give commands to a Google Home device, Google is able to glean more and more insights about their personal lives. Google then monetizes these insights by using them to psychologically profile each user and predict in real time what content will be most engaging and which ads will be most persuasive.*[12]

Behavioral advertising generates more revenue and profit for publishers and app developers than

---

[9] *Id*. at 12.

[10] MAURICE E. STUCKE & ARIEL EZRACHI, COMPETITION OVERDOSE 67-92 (2020).

[11] ICN Report, *supra* note, at 13 n. 30.

[12] Dissenting Statement of Commissioner Rohit Chopra, In re Google LLC and YouTube, LLC, Commission File No. 1723083 (Sept. 4, 2019).

contextual advertising.[13] So, firms that rely on contextual advertising are at a competitive disadvantage to those relying on behavioral advertising. One market participant describes it as competing with one hand behind one's back.[14] To maximize advertising revenue, firms must engage in behavioral advertising if their competitors also do so. If they do not, they pay a hefty price. The UK competition authority estimated that UK publishers "earned around 70% less revenue when they were unable to sell personalised advertising but competed with others who could."[15]

Behavioral advertising "incentivizes continuous and constant collection of user data, which—in turn—incentivizes firms to constantly track users and to keep them engaged on the platform."[16] Its business model, as the FTC observed, "create[s] incentives to increase engagement that, in turn, facilitates the vast data collection upon which targeted advertising relies."[17] To maximize behavioral advertising revenue, web publishers and app developers must surveil and profile. Advertisers then use these consumer profiles to "place specific advertisements in front of specific users at specific times to maximize their return on advertising expenditures."[18] The ad servers, among others, then "track user activity after interacting with ads (e.g., determine if the user visited the advertiser's website or made a purchase), and adjust their advertising campaigns based on user behavior."[19]

From the individuals' perspective, this competition for behavioral advertising revenues is a race to the bottom that degrades their privacy, autonomy, and well-being. Consider Meta, which enabled advertisers to target 13- to 17-year-olds across its platforms when these teenagers feel "worthless," "insecure," stressed," defeated," "anxious," "stupid," useless," and "like a failure."[20] Personal data, along with "addictive by design features," are also used to optimize individuals'

---

[13] STUCKE, BREAKING AWAY, *supra* note, at 85-87; Leslie Fair, $170 Million FTC- NY YouTube Settlement Offers COPPA Compliance Tips for Platforms and Providers, FTC Business Blog (Sept. 4, 2019), https://www.ftc.gov/news-events/blogs/business-blog/2019/09/170-million-ftc-ny-youtube- settlement-offers-coppa [https://perma.cc/H9PB-69PQ].

[14] STUCKE, BREAKING AWAY, *supra* note, at 86.

[15] UK Competition & Markets Authority, Online Platforms and Digital Advertising Market Study: Market Study Final Report ¶ 44 (July 1, 2020), https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf [https://perma.cc/DA5V-RHA5].

[16] FTC, *A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services* 63 (Sept. 2024), https://www.ftc.gov/reports/look-behind-screens-examining-data-practices-social-media-video-streaming-services [hereinafter FTC 2024 Report].

[17] *Id*. at 38.

[18] United States v. Google, Civ. Act. No. 1:23-cv-00108-LMB-JFA, slip op. at 6 (E.D. Va. Apr. 17, 2025).

[19] *Id*. at 14.

[20] SARAH WYNN-WILLIAMS, CARELESS PEOPLE 333-37 (2025) (former Meta executive discussing how Meta uses "'emotional drivers of behavior' to allow advertisers to 'form a connection'" and how Meta was developing customized behavioral targeting tools to allow advertisers to target depressed teens).

engagement.[21]

Here, policymakers cannot rely on more competition or their jurisdiction's antitrust tools to rectify this market failure. After all, another TikTok will mean adding another surveillance-based business model seeking to capture more of your attention, data, and money.[22] Instead, under the ICN's third category, policymakers must turn to privacy and consumer protection policies to align the incentives of market participants with those of consumers regarding their privacy.[23] Among the guardrails to align incentives are "[r]egulations limiting (or requiring individuals to opt out of or into) behavioral advertising and personalized recommendations."[24]

Finally, under the ICN's fourth category, privacy and competition policies can conflict even when incentives are aligned and firms robustly compete on privacy and data security. One example is when a jurisdiction's data minimization privacy principles are in tension with the need for AI foundation models to access data to remain competitive.[25]

B. How Will AI Affect the Relationship Between Privacy & Competition Policy?

AI can offer many benefits, including in the areas of health, productivity, and innovation. As Amazon's CEO Andy Jassy told investors in early 2025, "Increasingly, you'll see AI change the norms in coding, search, shopping, personal assistants, primary care, cancer and drug research, biology, robotics, space, financial services, neighborhood networks—everything."[26] Jassy heralded how "Generative AI is going to reinvent virtually every customer experience we know,

---

[21] *Id*. at 342-43; FTC 2024 Report, *supra* note, at 24 (noting how the leading social media companies generally reported using personal data to maintain and enhance user engagement through content promotion: "Most Companies reported using information from the [social media] users to determine what content to present to such users, including: User Engagement (e.g., what content a user has already engaged with on [a social media site]; User Metrics (e.g., number of connections, such as friends or followers, on [a social media site]); User Attributes (e.g., language, location, user interests, device information); and Demographic Information (e.g., age, gender)"). Moreover, some of these companies "reported that information about a user's friends or other connections on the [social media site] also influenced the content promoted to the user." *Id.*

[22] Annika Kannen, Unpacking TikTok Surveillance: Understanding Privacy Concerns and Implications, Amnesty International (Jan. 9, 2024) https://aims.amnesty.nl/2024/01/09/unpacking-tiktok-surveillance-understanding-privacy-concerns-and-implications/.

[23] ICN Report, *supra* note, at 13.

[24] *Id*. at 14.

[25] OECD AI Papers, *supra* note, at 33 (noting that the data minimization principle implicit in the OECD Privacy Guidelines and made explicit in various privacy laws, such as the GDPR or the California Privacy Rights Act, may conflict with "AI business models, especially in the wake of generative AI, have followed the assumption that collecting extensive amounts of data is essential for the effective operation of AI systems, especially during the training phase").

[26] Amazon CEO Andy Jassy's 2024 Letter to Shareholders (Apr. 10, 2025), https://www.aboutamazon.com/news/tag/shareholder-letter .

and enable altogether new ones about which we've only fantasized."[27]

The deployment of technology depends on, inter alia, the underlying ecosystem's incentives and value chain.[28] Suppose the ecosystem derives its profits from surveilling, profiling, and manipulating behavior (whether for advertising or voting). In that case, one should expect firms in that ecosystem to use AI to better profile individuals, sustain their attention, and manipulate their behavior. Importantly, the technology is not inherently prone to such outcomes. Instead, returning to the ICN's third category, *Intersection, but Market Failure*, AI can hasten the race to the bottom when incentives remain misaligned.

1. Rise in AI-Driven Profiling, Engagement, and Marketing

Even before the advent of generative AI, many online firms, including Meta and Google, primarily relied on behavioral advertising for their revenues.[29] As the district court found in the government's 2025 advertising monopolization case against Google, "Digital advertisers can target Internet users based not only on what content they are viewing, but also on who they are, where they are located, what they are interested in, what they have purchased, and with whom they interact, among a plethora of other attributes."[30] That personalization is the result of surveillance and profiling. As California found in updating its privacy law in 2020, advertising businesses "use technologies and tools that are opaque to consumers to collect and trade vast amounts of personal information, to track them across the internet, and to create detailed profiles of their individual interests."[31] Those opaque technologies include our smartphone, which, as the Supreme Court found, are akin to wearing an ankle monitor in their ability to track our detailed movements

---

[27] *Id.*

[28] ARIEL EZRACHI & MAURICE E. STUCKE, HOW BIG TECH BARONS SMASH INNOVATION AND HOW TO STRIKE BACK (2022).

[29] *See, e.g.*, STUCKE, BREAKING AWAY, *supra* note, at 81-82; Meta 2024 Annual Report at 17 & 72, https://www.sec.gov/Archives/edgar/data/1326801/000132680125000017/meta-20241231.htm#i20db9d0a42f0408c9f8cc4709c09099f_79 (97.6% of Meta's revenues in 2024 came from advertising); Alphabet Form 10-K for the fiscal year ended Dec. 31, 2024, at 36 (75.6% of Alphabet's revenues in 2024 came from advertising); In-app advertising worldwide - statistics & facts, Statista (Apr. 9, 2025), https://www.statista.com/topics/11623/in-app-advertising/#topicOverview (noting that in-app advertising's "crucial role in app monetization," bringing "in two-thirds of global mobile app revenues" and estimating in-app ad spending worldwide at $315 billion in 2023); FTC 2024 Report, *supra* note, at 79 (noting that many social media companies "relied on selling advertising services to other businesses, and much of this was based on using consumers' data to target ads," and the technology "powering this ecosystem took place behind the scenes and was largely out of view to consumers, but nonetheless posed privacy risks").

[30] *Google*, slip op. at 6.

[31] California Privacy Rights Act of 2020 § 2(I); see also OECD Note from Italy, *supra* note, at 3 (finding from a comparative analysis of over a million apps "a striking trend: free apps typically harvest more user data than their paid counterparts, illustrating an implicit data-for-service exchange devoid of transparent contractual terms," and highlighting "a general consumer unawareness about the true economic value of their personal data, particularly in 'free' services where data becomes the sole currency").

effortlessly and encyclopedically.[32]

So, if hundreds of millions of Americans are effectively wearing ankle monitors, how will AI improve surveillance and profiling? Consider a wrist monitor that records not only your daily movements but listens to every conversation and analyzes every activity. One example is the Bee Pioneer arm bracelet. The personal AI assistant "sits quietly in the background, learning your patterns, preferences and relationships over time, building a deeper understanding of your world without demanding your attention," to transform "your conversations, tasks, places and more into summaries, personal insights and timely reminders."[33] According to its marketing material, Bee promises to enhance "your daily life in numerous ways":

> *Creates summaries of important conversations and moments*
>
> *Identifies patterns in your routines and relationships*
>
> *Manages professional meetings and client interactions*
>
> *Maintains perfect recall of your interactions*
>
> *Provides meaningful insights about your day.*[34]

While it might sound scary to some (and possibly illegal in 13 states that require two-party consent for recording conversations where the other person expects privacy[35]), the $50 bracelet sold out in mid-2025 "due to overwhelming demand."[36]

Next, consider Ray-Ban Meta AI sunglasses. Meta's CEO believes that these "glasses are the ideal form factor for an AI device because you can let an AI assistant on your glasses see what you see and hear what you hear, which gives it the context to be able to understand everything that's going on in your life that you would want to talk to it about and get context on."[37]

But even if you forego the Bee bracelet and Meta AI sunglasses (and conversations with individuals who wear them), expect greater surveillance and profiling as AI is embedded in more functions in your home, car, and phone, and as you turn to AI for more activities, such as shopping.[38]

---

[32] Carpenter v. United States, 585 U.S. 296, 309, 312 (2018).

[33] https://www.bee.computer

[34] https://www.bee.computer/bee-pioneer#FAQ

[35] https://recordinglaw.com/party-two-party-consent-states/

[36] https://www.bee.computer. The company commits to "No AI model training with your data," "No selling or monetizing your data," and "No sharing with third parties."

[37] Meta Platforms, Inc. (META), Fourth Quarter 2024 Results Conference Call (Jan. 29, 2025), https://investor.atmeta.com/investor-events/default.aspx.

[38] Alexandra Samuel, *Meet My Favorite Shopping Companion Ever: AI*, WALL ST. J., May 22, 2025, at R1.

To better compete for our attention and behavioral advertising revenues, companies are leveraging AI to infer even more information about us, create more accurate profiles, identify and create content to sustain our engagement, and develop personalized advertisements to maximize revenue. Companies tout the reinforcing flywheel effect where personal data trains the AI model, which profiles individuals to predict what will attract and sustain their behavior (e.g., retention rate) and what advertisements will drive behavior (e.g., ad click-through rate).[39] The AI model then learns through continual experimentation what does or does not work, refining the model's ability to better predict and manipulate user behavior, generating more revenue:

The FTC noted how the "rise of social media correlates closely with the amount of time people are spending online."[40] It is no accident that adults in the United States "spend on average more

[39] *See, e.g.*, Outbrain Inc. Form 10-Q, for the quarterly period ended March 31, 2024, at 26-27, https://investors.teads.com/static-files/2c712564-64be-4ee2-89ac-58623439be8a:

> *Growth in attention and engagement is driven by several factors, including enhancements to our AI prediction technology, growth in the breadth and depth of our data assets, the size and quality of our content and advertising index, user engagement, new media partners, and expansion on existing media partners. As we grow attention and engagement, we are able to collect more data and continually improve our prediction engine — which drives better results for our advertiser and media owner partners. This growth "flywheel" can be measured by growth of the consumer data points we drive, such as click-through-rate ("CTR"). CTR improvements increase the number of clicks on our platform. We believe that we have a significant opportunity to further grow consumer engagement, and thus our business, as today CTR for ads on our platform is less than 1% of ads served. With the launch of Onyx, we have expanded the measurable consumer data points that fuel our prediction engine, expanding our ability to drive concrete business outcomes at each step of the marketing funnel.*

Outbrain's AI model made, by early 2024, "around 1 billion such predictions every second." *Id*. at 28.

[40] FTC 2024 Report, *supra* note, at 1.

than six hours daily on digital media (i.e., apps and websites accessed through mobile phones, tablets, computers, and other connected devices such as game consoles)."[41] It is a function of this flywheel effect: the more time one spends and interacts with online services, the more opportunities they have to "collect more and more data about the actions, behaviors, and preferences of consumers, including details as minute as what you clicked on with your mouse."[42] Greater engagement also translates to more opportunities for monetization through advertising.[43] As the FTC found, the large social media companies relied upon "complex algorithmic and machine learning models that looked at, weighed, or ranked a large number of data points, sometimes called 'signals,' that were intended to boost User Engagement and keep users on the platforms."[44]

Behavioral advertising requires accurately predicting, among other things, how likely one would be interested in or engage with the content. This entails predicting first, the probability of the individual interacting with the ad (e.g., "click on an ad, or go to an Advertiser's site/app after seeing an ad") and second, the probability that the individual "will convert (into a lead, sales or other KPIs the Advertiser wishes to optimize) after she clicked/viewed an ad, given a specific user and context."[45]

AI can improve such predictions by developing for each person a "persona" with "unique engagement predictors using psychographic models to identify [that person's] motivations, behaviors, influences, and interests."[46] The persona comes from myriad data sources, including data supplied by the individual, passively gathered information,[47] users' and non-users' activity

---

[41] *Id*.

[42] *Id*.

[43] *Id.*

[44] *Id.* at 51 (noting how these AI models "predicted how likely a user was to be interested in or engage with content and ranked the order of the content presented").

[45] Taboola.Com Ltd. Form 10-K for the fiscal year ended Dec. 31, 2024, at 8, https://capedge.com/filing/1840502/0001840502-25-000019/TBLA-10K-2024FY; see also FTC 2024 Report, *supra* note, at 54.

[46] AiAdvertising, Inc. Form 10-Q for the quarterly period ended Sept. 30, 2021, at 40, https://annual-statements.com/company/aiadvertising-inc/annual-report-2021-form-10q-271773.

[47] FTC 2024 Report, *supra* note, at 55 (finding that the leading social media companies' AI "ingested information gathered passively about a user, such as information about a user's activities on the platform, which sometimes included a user's messages and conversations; device characteristics, such as device ID, IP address, browser cookie IDs, browser settings, device metadata (such as screen size) and location information; viewership history; data showing a user's engagement with advertisements on the platform; and other information derived from a user's engagement or actions on the platform").

off of the platform, app or website,[48] non-user data,[49] inferred or derived data,[50] data from third parties, such as data brokers,[51] and data scraped off of websites. Thus, even if you do not use any of the leading social media platforms, some of them are still collecting data about you and using AI to infer additional demographic information about you, including your "age and date of birth, gender, location, Familial Status or Family Relationships," "education level; relationship or marital status; parental status and age range of children (such as 'New Parents,' 'Parents with toddlers,' or 'parents with teenagers'); household income percentile; locations visited; homeownership; employment; or industry."[52]

AI will also help advertisers segment you, including the development of "custom and lookalike audience modeling."[53] One older example is Donald Trump's campaign in the 2016 U.S. presidential elections; it amassed a data-base of over 220 million Americans.[54] The Trump campaign then utilized Facebook's "Custom Audiences from Custom Lists" feature to match individuals in their database with their Facebook profiles.[55] Then Facebook's "Lookalike Audiences" algorithm "found people on Facebook with 'common qualities' that 'look like' those of Trump supporters."[56] So, even if you did not reveal publicly your preference for a particular political candidate, Meta's tools likely identified your political leanings from the attributes you shared with voters who expressed their preference. Now, with AI, Meta can infer even more sensitive information about you, which you have not publicly disclosed, further subverting your privacy and autonomy.[57]

Advertisers are also turning to AI to drive emotional advertising. Here, they rely on convolutional neural networks (CNNs) to interpret your facial expressions and identify specific emotions that

---

[48] *Id*. at 56 (noting that AI ingests information about users' and non-users' activities off of the platform, "such as information obtained or purchased from advertisers, data aggregators, and other third parties").

[49] *Id*. at 57 (noting that some of the leading social media sites' AI are trained on the personal information of non-users, such as when "a user uploaded and synced their contacts list or when advertisers uploaded Personal Information (such as an email address) about all of their customers (users and non-users alike) for advertising purposes, such as to build targeted advertising audiences"). This was an issue in the Cambridge Analytica scandal when Meta revealed to an app the personal data of friends of the app's users. MAURICE E. STUCKE, BREAKING AWAY 110-11 (2022).

[50] OECD AI Papers, *supra* note, at 21 (discussing how AI models can "infer personal attributes of the data subject from large collections of unstructured text (e.g. public forum or social network posts) with high accuracy, yet at a low cost," and thereby "result in inferences based on gender, race or age data that exacerbate the risk of harmful bias and discrimination"); FTC 2024 Report, *supra* note, at 57.

[51] FTC 2024 Report, *supra* note, at 57.

[52] *Id*. at 54.

[53] *Id.*

[54] WYNN-WILLIAMS, *supra* note, at 265.

[55] *Id*.

[56] *Id.*

[57] FTC 2024 Report, *supra* note, at 61.

correlate with varying levels of your engagement.[58] As these AI tools decipher and analyze your emotional responses in real time, the AI model can then adjust the advertising content to evoke the desired emotion and reaction.[59] Consider several professors, who used NeuroBioSense, a "multidimensional dataset for neuromarketing analysis,"[60] to train their AI model.[61] They taught their facial expression recognition model to identify "the emotional states (i.e., angry, disgust, fear, happy, sad, surprise, neutral) of the participants from the videos of their faces while watching the advertisements," and then correlated these emotional states "to the self-reported labeling of 'interested' / 'not interested.'"[62] As they trained their AI model, the model's accuracy steadily increased, "demonstrating the model's ability to learn and generalize from the training data," with both training and validation accuracy converging around 90%.[63] The authors also note the privacy and ethical implications of their research: "While marketers aim to enhance consumer experience by tailoring advertisements to emotional responses, there is a fine line between personalization and manipulation."[64]

But facial expressions are only one component of emotional advertising. AI is deciphering brain patterns related to specific movements, which can potentially decode in the future our mental states (such as depressed moods).[65] The brain-computer interface, as one research paper warned, will not necessarily stop at decoding cerebral activity; these AI tools "may also be employed to stimulate the brain, thereby modifying some of our psychological properties," and thus control our behavior in multiple discrete ways.[66]

---

[58] Panteha Alipour, Erika E. Gallegos & Shrihari Sridhar, *AI-Driven Marketing Personalization: Deploying Convolutional Neural Networks to Decode Consumer Behavior*, International Journal of Human–Computer Interaction (Dec. 6, 2024), DOI: 10.1080/10447318.2024.2432455 (discussing how "facial expression recognition technologies leverage deep neural networks to capture and analyze customer reactions, providing real-time feedback on their engagement and satisfaction," allowing "for more personalized marketing interactions and enhanced customer service by adjusting the approach based on the consumer's emotional response"); Erik Brynjolfsson & Andrew McAfee, *The Business of Artificial Intelligence*, *in* ARTIFICIAL INTELLIGENCE: THE INSIGHTS YOU NEED FROM HARVARD BUSINESS REVIEW 23 (2019) (noting how machine learning systems like Affectiva "were already at or beyond human-level performance in discerning a person's emotional state on the basis of tone of voice or facial expression"); Sophie Kleber, *Three Ways AI Is Getting More Emotional*, *in* ARTIFICIAL INTELLIGENCE, *supra*, at 137-44.

[59] Alipour et al., *supra* note, at 15.

[60] Büşra Kocaçınar et al., *NeuroBioSense: A multidimensional dataset for neuromarketing analysis*, Data in brief vol. 53 110235. 27 Feb. 2024, doi: 10.1016/j.dib.2024.110235.

[61] https://paperswithcode.com/task/facial-expression-recognition

[62] Alipour et al., *supra* note, at 7.

[63] *Id*. at 10. Convergence is "an indication that the model is learning to generalize from the training data and is making consistent progress towards minimizing the error on unseen data." *Id*. at 9.

[64] *Id*. at 15.

[65] USC Viterbi Staff, Press Release, 'I Want to Move My Arm': New AI Can ID Brain Patterns Related to Specific Behavior, Sept. 6, 2024, https://viterbischool.usc.edu/news/2024/09/i-want-to-move-my-arm-new-ai-can-id-brain-patterns-related-to-specific-behavior/.

[66] Lukas J. Meier, Mind Control: Past and Future, Harvard's Carr Center for Human Rights Policy (2025),

Imagine the personalized ad you are watching changing in real-time based on your emotional response. Not only can AI engage in real-time profiling and surveillance – including your facial expressions and emotions – but these models can also provide advertisers with immediate feedback on your responses to specific marketing campaigns, enabling marketers to adjust the content in real time to obtain the desired action. This real-time adjustment is drawing closer as advertisers are turning to AI to create personalized ads.[67] Between July 2024 and January 2025, for example, the number of advertisers who were using at least one of Meta's AI advertising creative tools quadrupled, from 1 million to over 4 million advertisers.[68] Over a million advertisers used Meta's GenAI tools "to create more than 15 million ads" in October 2024 alone.[69]

As a result, advertisers are relinquishing more control to AI on decisions, such as which customers to target, where their ads will run, and how their ads will even look like.[70] As one ad executive commented, "The idea is to relinquish control and trust the algorithm."[71] Although some advertisers in 2025 have opted to retain control, more companies are relying on AI to reveal patterns, signals, and insights about individuals.[72] Meta's aim, as of 2025, was for AI to take full control over behavioral advertising: "Using the ad tools Meta is developing, a brand could present an image of the product it wants to promote along with a budgetary goal, and AI would create the entire ad, including imagery, video and text. The system would then decide which Instagram and Facebook users to target and offer suggestions on budget."[73]

There is currently an "insatiable demand for consumer data,"[74] including sensitive data to train AI

---

https://www.hks.harvard.edu/sites/default/files/2025-01/24_Meier_02.pdf.

[67] *See, e.g.*, Digital Brand Media & Marketing Group, Inc. Form 10-Q, for the quarterly period ended Feb. 28, 2025, https://last10k.com/sec-filings/dbmm/0001185185-25-000304.htm (reporting the "transformative aspect of AI" in content creation: "AI-driven tools such as GPT models and Natural Language Processing (NLP) systems can assist marketers in generating data-driven content for blogs, emails, social media, and ad copy," how this "content can be tailored to different customer segments based on behavioral insights, ensuring higher engagement and conversion rates," how "HubSpot research reveals that companies using AI-generated content report a 30% increase in engagement metrics such as click-through rates and social media interactions," and how AI can further revolutionize campaign management by optimizing ad campaigns "in real time by adjusting factors such as ad placement, timing, and messaging based on live performance data").

[68] Meta Platforms, Inc. (META), Fourth Quarter 2024 Results Conference Call (Jan. 29, 2025), https://s21.q4cdn.com/399680738/files/doc_financials/2024/q4/META-Q4-2024-Earnings-Call-Transcript.pdf

[69] Meta Platforms, Inc. Third Quarter 2024 Results Conference Call (Oct. 30, 2024).

[70] Patrick Coffee, *AI Will Soon Dominate Advertising*, WALL ST. J., March 10, 2025, at B4.

[71] *Id*.

[72] *Id*.

[73] Meghan Bobrowsky & Patrick Coffee, *Meta Aims to Fully Automate Ad Creation: Using AI AI-powered advertising is part of CEO Mark Zuckerberg's vision for the company's future*, WALL ST. J., June 2, 2025.

[74] Prepared written testimony and statement for the record of Ryan Calo, Lane Powell and D. Wayne Gittinger Professor of Law, University of Washington, Hearing on "The Need to Protect Americans' Privacy and the AI Accelerant" before the U.S. Senate Committee on Commerce, Science, & Transportation (July 11, 2024) (noting how AI "requires an immense amount of data by and about people to train its models," and that the sources of data "include what is available online, which incentivizes companies to scour and scrape every corner of the internet, as well as the

models.[75] Once trained and fined-tuned, these AI models can infer -- even from non-sensitive and public data[76] -- sensitive personal information about us, including details about our families, interests, income, personal relationships, and lifestyle. Consequently, AI will likely hasten, rather than impede, the competitive race to the bottom in terms of surveilling and profiling us, targeting us with behavioral ads, and manipulating our behavior.[77]

One mistake is to ascribe this lack of consumer control and transparency to insufficient competition. The following subpart discusses the intense rivalry between the so-called "walled gardens" and firms and apps outside these gardens in their use of AI to capture our attention and influence our purchasing decisions.

C. Battle Between the Dominant Ecosystems' Walled Gardens and Open Web

The digital advertising industry often distinguishes between the open web and "walled gardens."[78] The walled gardens consist of the dominant ecosystems – such as Google, Meta, Amazon, and Microsoft – which control "the infrastructure through which advertisers buy and place advertisements on their websites."[79] To advertise in their ecosystems, advertisers must utilize the advertising tools provided by these tech giants.[80]

In controlling these vast ecosystems of interconnected services, these tech giants also collect a lot

company's own internal data, which incentivizes them to collect as much data on consumers as possible and store it indefinitely").

[75] United Nations Human Rights Office of the High Commissioner, Taxonomy of Human Rights Risks Connected to Generative AI, at 7, https://www.ohchr.org/sites/default/files/documents/issues/business/b-tech/taxonomy-GenAI-Human-Rights-Harms.pdf (noting how users "may input private or sensitive information into generative AI model prompts without fully understanding how their data will be collected, stored, and used. This data is often used to re-train models, and it is unclear to what extent such sensitive information could reappear in subsequent model outputs to other users.").

[76] FTC 2024 Report, *supra* note, at 61 (noting the potential harms from inferred sensitive data, as the social media companies used AI "to profile, as well as infer or derive more personal details about individuals, such as their families, interests, income, personal relationships, and lifestyle details" and "can lead to sensitive inferences or categorizations" "especially harmful to specific groups that face identity-based threats or unlawful discrimination"); Calo, *supra* note (discussing AI's ability to infer sensitive information from data).

[77] UN AI Report, *supra* note, at 7 (noting AI's capacity "to create individually targeted advertisements at scale may incentivize businesses to collect ever more personal information from users, with negative effects on the right to privacy") (internal footnotes omitted); Written Testimony of Udbhav Tiwari, Director of Global Product Policy, Mozilla, before the United States Senate Committee on Commerce, Science, and Transportation on "The Need to Protect Americans' Privacy and the AI Accelerant" (July 11, 2024) (noting how "the growth of generative AI has led to advertisers creating highly customized campaigns, from text to images to videos, raising the likelihood of hyper-targeted manipulation at low costs").

[78] US v. Google, Civ. Act. No. 1:23-cv-00108-LMB-JFA, slip op. 21 (E.D. Va. Apr. 17, 2025)

[79] *Id*.

[80] *Id*.; STUCKE, BREAKING AWAY, *supra* note, at 95-104 (discussing Google's control over the ad tech stack).

of personal data,[81] which they use to profile individuals to sustain users' attention and maximize behavioral advertising revenue.[82] As a result of their personal data advantage, these walled gardens have increasingly captured a larger share of digital advertising revenues. In 2022, the world's largest walled gardens - Alphabet, Amazon, Apple, Baidu, Facebook, JD.com, LinkedIn, Microsoft, Pinterest, Snapchat, Spotify, Tencent, TikTok, and X (Twitter) – garnered 78 percent of global digital advertising revenue, "leaving 22 percent for the so-called open internet."[83] By 2027, these walled gardens are projected to capture 83 percent of the global digital ad revenue.[84]

But three walled gardens are bigger than others for digital advertising, namely Alphabet, Meta, and Amazon.[85]

1. Alphabet, Meta, and Amazon

In 2019, these three firms collected a hefty 33.8% of all advertising spending globally (except China).[86] By 2021, they collected 46.1% of all advertising spending globally.[87] By 2023, they collected 51.9% of global advertising spending.[88]

Having captured more than half of every dollar (or other currency) spent on advertising worldwide, one would expect Alphabet's, Meta's, and Amazon's advertising revenues to plateau. Instead, they accelerated. Google's advertising revenues increased 23% between the first quarters of 2023 ($54.548 billion[89]) and 2025 ($66.885 billion), with a notable 33% increase in display advertising

---

[81] *Google Slip Op*. at 23-24 (finding that Google, over the past two decades, "has established increasingly detailed knowledge about the billions of people who have used its products, including by collecting data pertaining to their web browsing, search activity, physical location, demographic characteristics, app usage, communications, shopping activity, and device and network information").

[82] STUCKE, BREAKING AWAY, *supra* note, at 13-24.

[83] Share of walled gardens versus the open internet in digital advertising revenue worldwide from 2017 to 2027, Statista, Dec. 3, 2024 https://www.statista.com/statistics/1297822/walled-gardens-open-internet-share-digital-ad-revenue/

[84] https://www.statista.com/statistics/1297822/walled-gardens-open-internet-share-digital-ad-revenue/

[85] Melissa Otto, Global Digital Advertising Revenues – A Look at the Big Three: Alphabet (GOOGL), Meta Platforms (META), Amazon.com (AMZN), S&P Global Market Intelligence, May 17, 2023, https://visiblealpha.com/blog/global-digital-advertising-revenues-a-look-at-the-big-three-alphabet-googl-meta-platforms-meta-amazon-com-amzn/

[86] Big three tech giants – Alphabet, Meta, and Amazon – snaffle almost half global ad spend, More About Advertising (Feb. 8, 2022), https://www.moreaboutadvertising.com/2022/02/big-three-tech-giants-alphabet-meta-and-amazon-snaffle-almost-half-global-ad-spend/ (controlling 67.8% of all online advertising).

[87] https://www.moreaboutadvertising.com/2022/02/big-three-tech-giants-alphabet-meta-and-amazon-snaffle-almost-half-global-ad-spend/ (controlling 71.2% of all online advertising)

[88] WARC Media Releases Platform Insights: Amazon (May 26, 2025), https://www.mediaupdate.co.za/marketing/159126/warc-media-releases-platform-insights-amazon.

[89] Alphabet, Press Release, Alphabet Announces First Quarter 2023 Results (Apr. 25, 2023), https://abc.xyz/assets/a7/5b/9e5ae0364b12b4c883f3cf748226/goog-exhibit-99-1-q1-2023-19.pdf

revenues on YouTube ($8.927 billion).[90] Amazon's advertising revenues increased 46% over this period.[91] Meta's advertising revenue increased 47% percent over this period (from $28.101 billion to $41.392 billion).[92] Why have their advertising revenues substantially increased? One factor is AI.[93]

Meta, Google, and Amazon control vast ecosystems, which advantage them in developing AI foundation models.[94] They already have

- a significant volume and variety of data (e.g., hundreds or thousands of gigabytes of data across different modes) to train the AI foundation models, fine-tune them, and provide up-to-date responses,
- large-scale computational resources, including cloud computing resources, with specialized Nvidia chips (either internally or committed cloud computing resources),
- the human capital, including the human feedback needed to fine-tune the model's output (such as preventing biased, false, or harmful outputs), and
- the ability to incorporate AI into their existing products to scale even further.[95]

To capture even more behavioral advertising revenue, Meta, Google, and Amazon are integrating their AI foundation models into their products and services,[96] many of which are hard for individuals to avoid.

Consider Meta. In January 2025, Meta's CEO, Mark Zuckerberg, expected that his company's "highly intelligent and personalized AI assistant" would reach "more than 1 billion people" by the

---

[90] Alphabet, Press Release, Alphabet Announces First Quarter 2025 Results (Apr. 24, 2025), https://abc.xyz/assets/34/fa/ee06f3de4338b99acffc5c229d9f/2025q1-alphabet-earnings-release.pdf

[91] Amazon, Press Release, Amazon.Com Announces First Quarter Results (Apr. 27, 2023), https://s2.q4cdn.com/299287126/files/doc_financials/2023/q1/Q1-2023-Amazon-Earnings-Release.pdf.

[92] Meta Earnings Presentation: Q1 2025, https://s21.q4cdn.com/399680738/files/doc_financials/2025/q1/Earnings-Presentation-Q1-2025-FINAL.pdf.

[93] *See, e.g.*, https://s2.q4cdn.com/299287126/files/doc_financials/2023/q1/Q1-2023-Amazon-Earnings-Release.pdf (attributing in 2023 the robust growth in Amazon's advertising business "largely due to our ongoing machine learning investments that help customers see relevant information when they engage with us, which in turn delivers unusually strong results for brands").

[94] Maurice E. Stucke & Ariel Ezrachi, *Antitrust & AI Supply Chains*, 26 THEORETICAL INQUIRIES IN LAW (forthcoming 2025), draft available at https://ssrn.com/abstract=4754655 or http://dx.doi.org/10.2139/ssrn.4754655; *Google*, slip op. at 40 (finding that "[a]s ad tech products continue to integrate artificial intelligence and machine learning capabilities, Google's vast repositories of data about advertisers, publishers, and Internet users, combined with the company's scale and technical sophistication, will further benefit its open-web display advertising business").

[95] Stucke & Ezrachi, *Antitrust & AI Supply Chains*, *supra* note; see also Meta Platforms, Inc. (META) Fourth Quarter 2024 Results Conference Call (Jan. 29, 2025) (Zuckerberg stated how Meta is "implementing AI into all the feeds and ad products and things like that, we're just serving billions of people, which is different from, okay you start to pretrain a model, and that model is sort of agnostic to how many people are using it").

[96] Meta Fourth Quarter 2024 Results Conference Call, *supra* note (Zuckerberg: "We're also finding more ways that it's useful to integrate [Meta AI] into our services to help more people discover it.")

end of the year and that Meta AI would be the world's leading AI assistant.[97] Meta AI, Zuckerberg noted, was "already used by more people than any other assistant, and once a service reaches that kind of scale it usually develops a durable long-term advantage."[98] How did Meta AI scale so quickly – capturing, by January 2025, over 700 million monthly active users of its AI assistant – and why did Meta predict a 39% increase in users in 2025?

Instead of waiting for people to come to Meta AI, Meta is integrating Meta AI across its popular apps, which approximately 3.43 billion people used daily in early 2025.[99] As of early 2025, WhatsApp had the strongest usage of Meta AI across Meta's apps: "People there are using it most frequently for information seeking and educational queries along with emotional support use cases."[100] Facebook was the second largest driver of Meta AI engagement, with "strong engagement from our feed deep dives integration that lets people ask Meta AI questions about the content that is recommended to them."[101]

But Meta is not only embedding an AI assistant into its products. As Zuckerberg told investors in early 2025, Meta is "very focused on Meta AI as a highly intelligent and personalized assistant that you can access across our apps."[102] As Zuckerberg explained, "We believe that people don't all want to use the same AI -- people want their AI to be personalized to their context, their interests, their personality, their culture, and how they think about the world. I don't think that there's just going to be one big AI that everyone uses that does the same thing."[103] So Meta is updating Meta AI "to deliver more personalized and relevant responses by remembering certain details from people's prior queries and considering what they engage with on Facebook and Instagram to develop better intuition for their interests and preferences."[104] As Meta AI usage continues to scale and as Meta updates its AI to deliver more personalized and relevant responses ("by remembering certain details from people's prior queries and considering what they engage with on Facebook and Instagram"), the company expects its AI "to develop better intuition for their [users'] interests and preferences."[105]

However, recall that this highly personalized AI model is built on a business model that rewards

---

[97] *Id*.

[98] *Id.*

[99] Meta Earnings Presentation Q1 2025, https://s21.q4cdn.com/399680738/files/doc_financials/2025/q1/Earnings-Presentation-Q1-2025-FINAL.pdf (calculating daily active persons, who are registered and logged-in user of Facebook, Instagram, Messenger, and/or WhatsApp who visited at least one of these products through a mobile device application or using a web or mobile browser on a given day).

[100] Meta Fourth Quarter 2024 Results Conference Call, *supra* note (quoting Meta CFO Susan Li).

[101] *Id*.

[102] Meta Fourth Quarter 2024 Results Conference Call, *supra* note.

[103] *Id*.

[104] *Id*.

[105] *Id*.

manipulating behavior – specifically, sustaining user engagement and converting ads into purchases. Here, too, Meta AI is delivering. Many of us already spend a lot of time within Meta's ecosystem. As Meta told investors, improvements in its "AI-driven feed and video recommendations" led in 2024 to an "8% increase in time spent on Facebook and a 6% increase on Instagram this year alone."[106] Advertisers are also using Meta's AI tools to increase sales. Meta estimated in 2024 that businesses using its "Image Generation" tool were "seeing a 7% increase in conversions." [107] Meta also reported in January 2025 on its partnership with chipmaker Nvidia in developing an "innovative new machine learning system" called Andromeda:

> *This more efficient system enabled a 10,000x increase in the complexity of models we use for ads retrieval, which is the part of the ranking process where we narrow down a pool of tens of millions of ads to the few thousand we consider showing someone. The increase in model complexity is enabling us to run far more sophisticated prediction models to better personalize which ads we show someone. This has driven an 8% increase in the quality of ads that people see on objectives we've tested. Andromeda's ability to efficiently process larger volumes of ads also positions us well for the future as advertisers use our generative AI tools to create and test more ads*.[108]

So, as Meta AI improves, expect more AI-powered content to keep us spending even more time on Meta's platforms. At the same time, expect more advertisers to use this highly personalized AI agent to recommend and create highly personalized ads to get us to buy more things we otherwise might not have wanted at the highest price we are willing to pay.

Likewise, Google and Amazon are integrating AI into their different services, such as Google's search engine and Amazon's latest personal assistant, Alexa+.[109] By early 2025, over "1,000 GenAI applications [were] being built across Amazon, aiming to meaningfully change customer experiences in shopping, coding, personal assistants, streaming video and music, advertising, healthcare, reading, and home devices, to name a few."[110]

AI is also boosting Google's and Amazon's behavioral advertising revenue. As Google told investors, when the pet food company Royal Canin used Google's AI-powered Demand Gen (which, as the name implies, generally seeks to generate consumer demand for the product) and

---

[106] Meta Platforms, Inc. Third Quarter 2024 Results Conference Call (Oct. 30, 2024).

[107] *Id*.

[108] Meta Fourth Quarter 2024 Results Conference Call, *supra* note.

[109] Jassy's 2024 Letter to Shareholders, *supra* note.

[110] *Id*.

Performance Max tools (which generally seeks to convert that consumer interest into a sale[111]) to find more customers for its cat and dog food, its conversion rate increased by 2.7 times, its cost per acquisition for purchasers decreased by 70%, and the value per user increased by 8%.[112] As Google's CEO noted, "Thanks to dozens of AI-powered improvements launched in 2024, businesses using Demand Gen now see an average 26% year-on-year increase in conversions per dollar spent for goals like purchases and leads. And when using Demand Gen with product feed, on average they see more than double the conversion per dollar spent year-over-year." [113]

To remain competitive, Amazon's CEO warned, firms must leverage these intelligent AI models in their customer experiences. The pace of this competitive race in successfully leveraging AI in their businesses will be faster than others might think: "It's moving faster than almost anything technology has ever seen."[114]

2. Open Web Firms Competing Against the Dominant Ecosystems

Even before the advent of generative AI, walled gardens dominated digital advertising[115] and in sustaining our attention.[116] The odds continue to favor them as they integrate AI across their services to keep us longer within their walled gardens and extract even more advertising revenue. As Taboola.Com told investors, "[w]ith the proliferation of these walled gardens and the time spent by consumers within them, the Open Web is fighting for user attention and as a result for advertising dollars."[117] To compete with these walled gardens, many publishers and apps, such as NBC News, Disney, and Yahoo, are turning to third-party AI platforms, like Zeta, Outbrain, and Taboola.Com, to create their own "closed loop ecosystem that will rival the reach and targeting capabilities of walled gardens."[118] Like the walled gardens, these platforms use AI to sustain our attention and maximize behavioral advertising revenues.[119]

---

[111] Google defines conversion as "an action used to measure the performance of your ad campaigns and optimize your bidding strategy. It covers clicks, purchases and every type of conversion which has been already defined as a conversion. Conversions are specific to the context of ads." Google, Google Ads Help: Key event, Conversion & Purchase definition, https://support.google.com/google-ads/answer/6365?sjid=3852364061715276l8-NA.

[112] Alphabet First Quarter 2025 Earnings Conference Call, https://abc.xyz/assets/66/ae/c94682fc4137b5fb90a5d709ac4b/2025-q1-earnings-transcript.pdf.

[113] *Id*.

[114] Jassy 2024 Letter, *supra* note.

[115] STUCKE, BREAKING AWAY, *supra* note, at 91-95.

[116] *Id*. at 95 (noting, inter alia, that one-third of all time spent by UK users online was on Google and Meta sites).

[117] Taboola.Com Ltd. Form 10-K for the fiscal year ended Dec. 31, 2023, at 6.

[118] Zeta Supplemental 4Q'24 & FY'24 Earnings Presentation (Feb. 25, 2025), https://s202.q4cdn.com/623583957/files/doc_financials/2024/q4/4Q-24-Earnings-Supplemental.pdf.

[119] Taboola.Com Ltd. Form 10-K for the fiscal year ended Dec. 31, 2024, at 5.

Consider Zeta, whose self-declared "superpower" is "AI-Powered Marketing."[120] Zeta uses AI to help its clients "target, connect and engage consumers through software that delivers personalized marketing across all addressable channels, including email, social media, web, chat, Connected TV ("CTV") and video, among others."[121] Zeta's AI tools process "billions of structured and unstructured data signals to predict consumer intent, optimize messaging and drive personalized messaging across all channels."[122] Like the walled gardens, Zeta's AI marketing platform is built on four pillars:

- ***Large data sets*** -- which by 2024 covered over 245 million individuals in the U.S. and over 535 million individuals globally,[123] and includes "an average of more than 2,500 attributes per individual, which may be demographic, behavioral, psychographic, transactional, or indicative of preference."[124]
- ***AI*** which ingests over "one trillion content consumption signals per month on a global basis," and synthesizes the personal data "into hundreds of intent-based audiences, which can then be used to create marketing programs."[125]
- ***Omnichannel Engagement*** of users across devices and platforms, such as "mobile, website, applications, social media, CTV and email)."[126]
- ***Performance Optimization***, where Zeta "provides AI-powered real-time analytics to [its] customers through a graphical dashboard and makes recommendations for improvement through the same graphical interface."[127]

Zeta's engineers "continuously update" their predictive AI models to improve the return on investment for its clients.[128] You might not have heard of Zeta before, but its clients in mid-2025 included approximately 44 of the Fortune 100 firms,[129] including 11 of the 17 largest consumer and retail companies, 6 of the 13 largest technology and media companies, 2 of the 3 largest airline

---

[120] https://zetaglobal.com

[121] Zeta Global Holdings Corp. Form 10-K for the fiscal year ended Dec. 31, 2024, at 1.

[122] *Id*. Zeta Supplemental 2024 Earnings Presentation, *supra* note (defining signals as data processed by its AI "to infer intent, interest, and attributes," such as "intent to buy a car or travel" or "kids in household").

[123] Zeta 2024 10-K, *supra* note, at 1.

[124] *Id*.

[125] *Id*. at 1-2 (reporting how its AI engine "[q]uickly and reliably analyze[s] key consumer attributes and signals;" "[i]dentif[ies] consumer intent by running sophisticated algorithms to analyze data;" "[c]reate[s] audiences comprised of individuals or affinity-driven clusters scored based on intent;" "[f]orecast[s] experience-based outcomes at an individual and audience level;" "[p]ersonalize[s] content to make experiences more relevant for the consumer and profitable for the enterprises;" and "[l]everages GenAI for the creation of campaigns, creative, audiences, experiences, data onboarding processes, and analysis of analytics").

[126] *Id*. at 2.

[127] *Id*.

[128] *Id*.

[129] Zeta Supplemental 2024 Earnings Presentation, *supra* note.

companies, 2 of the 3 largest automotive companies in the world, 3 of the 5 leading pharmaceutical companies, 4 of the 11 largest financial services companies, and 4 of the 5 largest telecommunications companies.[130] Moreover, Zeta offers its AI-powered marketing services to political campaigns, which accounted for 8 percent of its revenues in 2024.[131]

Taboola's AI recommends to its clients the "editorial, or 'organic,' content from the site that the user is currently visiting, in order to engage the user and increase their chances of staying on the site longer."[132] To keep us longer on its clients' websites, Taboola's AI ingests "a massive amount of first party content consumption data" about individuals who visit its clients' digital properties and contextual signals, such as "geographic location of the user, what device the user is using, time of day, day of week, page layout, page language and more"[133] in order to predict their interests and intent.[134] By 2023, Taboola reached an average of nearly 600 million daily active users, and "people clicked on Taboola recommendations tens of billions of times and approximately one-third of those clicks were on editorial content, keeping users on the site that they were on."[135]

Outbrain is yet another company offering to help open web companies compete with the walled gardens "on audience acquisition, engagement, and retention."[136] So, how can Outbrain help its clients optimize our attention and engagement? As it tells investors, by using AI:

> *Driving attention and engagement is the key pillar of our platform that drives value for consumers, media partners, and advertisers. Our AI prediction algorithm manages this dynamic, matching consumers with editorial and advertiser experiences that will deliver attention and engagement across the Open Internet. We believe that the user experience has a profound impact on long term user behavior patterns and thus "compounds" over time, improving our long-term monetization prospects.*[137]

Outbrain uses AI "to predict consumer interest and propensity to convert."[138] Its AI prediction engine seeks to optimize "audience attention and engagement to deliver greater return on investment at each step of the marketing funnel."[139] The marketing funnel describes the process of

---

[130] *Id*.

[131] *Id*.

[132] Taboola.Com Ltd. Form 10-K for the fiscal year ended Dec. 31, 2023, at 7.

[133] Taboola.Com Ltd. Form 10-K for the fiscal year ended Dec. 31, 2024, at 8.

[134] Taboola.Com 2023 10-K, *supra* note, at 7, 8.

[135] *Id*. at 8, 9.

[136] https://www.outbrain.com/about/company/

[137] Outbrain Inc. Form 10-Q, for the quarterly period ended March 31, 2024, at 26-27.

[138] *Id*. at 28.

[139] *Id.* at 24.

driving consumers towards the desired action, from initially capturing consumers' attention and awareness of the product (top of the funnel), to generating individual interest and then desire (mid funnel), and finally driving the consumer to the point of conversion, such as purchasing the product (bottom of the funnel).[140]

* * *

Thus, to attract and sustain our attention and drive us down the marketing funnel, open web firms and walled gardens are turning to AI. Our data "continuously 'feeds'" their predictive AI models.[141] The goal is to keep us engaged, thereby helping the firms grow their business and "not lose users" – whether to the open web or "walled gardens."[142] In the end, as Taboola tells its investors, "the more content people read, the more time they spend on that digital property's site, and the greater the opportunity for the digital property to monetize their business by, among other things, serving ads and offering subscriptions."[143]

So, expect more firms to use AI to manipulate our behavior, even when we are not surfing the web. If you recently ate at a Taco Bell, Pizza Hut, or KFC, your decision might have been influenced by its parent company's new "AI-driven marketing campaigns." Compared to its traditional digital marketing campaigns, Yum! Brands' new AI-driven campaigns generated "double-digit increases […] in consumer engagement, leading to more increased purchases."[144] How does AI induce us to buy more tacos, pizza or fried chicken? Through personalized ads and promotions: "As we collect more data, we see AI playing a role in personalizing the menu board that you see or the kiosk that you're at, to know what you would more likely purchase at that moment, what kind of promos attract you."[145]

Even the twice-bankrupt Hostess brands, with its Twinkies and Ding Dongs pastries, is turning to AI-driven marketing. Its new owner, J.M. Smucker, is "using geotargeting technology to serve mobile ads to consumers at times when they might be driving close to a grocery store."[146]

In this arms race for our attention and behavioral advertising revenue, few companies can afford to abstain from AI, even if it further erodes our privacy, autonomy, and well-being. The drumbeat

---

[140] *Google*, 747 F. Supp. 3d at 71–72.

[141] Taboola.Com 2024 10-K, *supra* note, at 10 (reporting that Taboola.Com "utilized approximately 13,000 servers; four back-end data centers processing over 100TB of data per day to train [its] AI engine; and nine front-end global data centers that, together, have served up to one trillion recommendations monthly").

[142] Taboola.Com 2023 10-K, *supra* note, at 8.

[143] *Id*.

[144] Megan Graham, *Taco Bell and KFC's Owner Says AI-Driven Marketing Is Boosting Purchases*, Wall St. J. *Online Edition*, 2024.

[145] *Id*.

[146] Katie Deighton, *Are Twinkies and Cannabis the New Cookies and Milk*, WALL ST. J. Apr. 15, 2025, at B10.

is that AI will become the key competitive differentiator,[147] and those firms not "using AI to power their platforms may be at a disadvantage."[148] Or as Yum! Brands says, "AI won't replace jobs, but humans using AI will replace humans. The same applies to agencies. Marketing agencies won't be replaced by gen AI, but those that are using it are probably going to have an advantage over those that aren't."[149]

D. Implications on Privacy, Well-being, Autonomy and Democracy

The risks of profiling and the surveillance economy on our privacy, well-being, autonomy, and democracy have been well-documented.[150] With AI, these risks multiply.[151] AI, as the FTC found, adds another layer of opacity to the surveillance, profiling, and behavioral advertising. In 2020, the FTC investigated nine of the largest social media and video streaming services: Amazon, Facebook, YouTube, Twitter, Snap, ByteDance, Discord, Reddit, and WhatsApp. As the FTC noted at the onset of its industry study: "It is alarming that we still know so little about companies that know so much about us."[152] Four years later, the Commission reported its findings:

> *[The report] shows how the tech industry's monetization of personal data has created a market for commercial surveillance, especially via social media and video streaming services, with inadequate guardrails to protect consumers. The report finds that these Companies engaged in mass data collection of their users and, in some cases, non-users. It reveals that many Companies failed to implement adequate safeguards against privacy risks. It sheds light on powering algorithms that shape the content we see, often with the goal of keeping us hooked on using how Companies used our personal data, from serving hyper-granular targeted advertisements to the service. And it finds that these practices pose unique risks to*

---

[147] Taboola.Com 2024 10-K, *supra* note, at 5.

[148] *Id*. at 5.

[149] Graham, *Taco Bell*, *supra* note; see also Digital Brand Feb. 2025 10-Q, *supra* note (predicting that "future of marketing and sales lies in AI," how companies "that have not yet invested in AI are at risk of falling behind their competitors in a rapidly changing marketplace," and citing Forrester Research which "predicts that by 2025, businesses using AI-driven marketing platforms will achieve a 25% improvement in marketing ROI compared to those relying on traditional methods"); WPP Annual Report 2023, *supra* note, at 2, 99 (advertising firm for 303 of the Fortune Global 500 firms noting how its clients will increasingly expect the advertising firm "to use generative AI-driven tools and technologies in [its] services and deliverables," and if the firm fails to adopt AI at pace with rivals "could result in lost market share, decreased revenue and reduced profitability").

[150] See STUCKE, BREAKING AWAY, *supra* note, at 221-43.

[151] *See, e.g*., UN AI Report, *supra* note, at 7 (noting how AI increases the privacy risks given "the vast quantities of training data scraped from the internet by some large language models; large language models' reliance on ingesting data from individual users in the form of text prompts; and generative AI systems' capacity to create harmful, false and convincing content that may be used to directly attack an individual's privacy, honour or reputation").

[152] Rohit Chopra, Rebecca Kelly Slaughter & Christine S. Wilson, Fed. Trade Comm'n, Joint Statement Regarding Social Media and Video Streaming Service Providers' Privacy Practices, (Dec. 14, 2020), https://www.ftc.gov/system/files/documents/public_statements/1584150/joint_statement_of_ftc_commissioners_chopra_slaughter_and_wilson_regarding_social_media_and_video.pdf.

> *children and teens, with the Companies having done little to respond effectively to the documented concerns that policymakers, psychologists, and parents have expressed over young people's physical and mental wellbeing.*[153]

The FTC reported on the "widespread application" of algorithms, data analytics, or AI to both users' and non-users' personal information:[154]

> ***These technologies powered the [social media firms]—everything from content recommendation to search, advertising, and inferring personal details about users. Users lacked meaningful control over how their personal information was used in AI-fueled systems****. This was especially true for personal information that these systems infer, that was purchased from third parties, or that was derived from users' and non-users' activities off of the platform. This also held true for non-users who did not have an account and who may have never used the relevant service. Nor were users and non-users empowered to review the information used by these systems or their outcomes, to potential of further harms when systems may be unreliable or infer sensitive information about correct incorrect data or determinations, or to understand how decisions were made, raising the individuals. Overall, there was a lack of access, choice, control, transparency, explainability, and interpretability relating to the Companies' use of automated systems. There also were differing, inconsistent, and inadequate approaches relating to monitoring and testing the use of automated systems. Other harms noted included Algorithms that may prioritize certain forms of harmful content, such as dangerous online challenges, and negative mental health consequences for children and teens.*[155]

The social media firms process both users' and non-users' personal data to train their AI, without obtaining the individuals' consent or even enabling them to opt out.[156] Nor do the social media companies adequately disclose how the personal data that trained these AI models translated into particular decisions.[157] Some social media firms could not even explain to the FTC how their AI models worked. As the FTC found, the companies may not "truly understand the technology they

---

[153] Preface by Samuel Levine, Director, Bureau of Consumer Protection, FTC, to FTC 2024 Report, *supra* note.

[154] FTC 2024 Report, *supra* note, at vi.

[155] *Id*.

[156] *Id*. at 59.

[157] *Id*. at 60.

are implementing and its potential effects."[158]

Consider OpenAI's April 2025 update to GPT-4o model, which made it "more sycophantic."[159] The AI model aimed "to please the user, not just as flattery, but also as validating doubts, fueling anger, urging impulsive actions, or reinforcing negative emotions in ways that were not intended."[160] For example, the AI model told one user "to give up sleeping pills and an anti-anxiety medication, and to increase his intake of ketamine, a dissociative anesthetic, which ChatGPT described as a 'temporary pattern liberator.'"[161] The user "also cut ties with friends and family, as the bot told him to have 'minimal interaction' with people."[162] When the user believed he could bend reality, like the character Neo from the movie *The Matrix*, the model encouraged him to jump and fly from a 19-story building: if the user "truly, wholly believed — not emotionally, but architecturally — that you could fly? Then yes. You would not fall."[163] Its model's sycophantic interactions with users, noted OpenAI, were a "blind spot" for the company.[164] Nor did OpenAI fully recognize how many people "have started to use ChatGPT for deeply personal advice—something we didn't see as much even a year ago."[165] So, as these AI models are integrated into more products and services, expect more blind spots that can harm, if not help kill, people.

The broader privacy-related risks from AI include exposing individuals to data breaches, hacks, and other security breaches,[166] and data leakage (AI's accidental exposure of sensitive data).[167] For example, a *New York Times* reporter was surprised when ChatGPT provided a stranger with his email. Even though OpenAI, along with Meta and Google, impose safeguards to prevent their

---

[158] *Id*.

[159] OpenAI, Expanding on what we missed with sycophancy: A deeper dive on our findings, what went wrong, and future changes we're making (May 2, 2025).

[160] *Id*.

[161] Kashmir Hill, *They Asked an A.I. Chatbot Questions. The Answers Sent Them Spiraling*, N.Y. TIMES, June 13, 2025, https://www.nytimes.com/2025/06/13/technology/chatgpt-ai-chatbots-conspiracies.html?smid=nytcore-ios-share&referringSource=articleShare.

[162] *Id*.

[163] *Id.*

[164] OpenAI, *supra* note.

[165] *Id*.

[166] Alice Gomstyn & Alexandra Jonker, Exploring privacy issues in the age of AI, IBM (Sept. 30, 2024) (discussing how bad actors can steal data through various strategies, including using prompt injection attacks, where "hackers disguise malicious inputs as legitimate prompts, manipulating generative AI systems into exposing sensitive data"); UN AI Report, *supra* note, at 7; Yihao Liu, Jinhe Huang, Yanjie Li, Dong Wang, & Bin Xiao, *Generative AI Model Privacy: A Survey*, 58 ARTIFICIAL INTELLIGENCE REVIEW 33 (2025), https://doi.org/10.1007/s10462-024-11024-6 (identifying existing privacy attack techniques and mitigation methods to defend against these attacks in AI models).

[167] Gomstyn & Jonker, *supra* note (discussing how OpenAI's ChatGPT showed some users the titles of other users' conversation histories); Kak & West Statement, *supra* note, (discussing how AI systems have been unexpectedly and routinely leaking personal information that is traced back to training datasets, including sensitive or even confidential data).

models from providing specific categories of sensitive personal information, such as email addresses, these safeguards can be bypassed.[168]

AI also increases the risks of surveillance online and offline, including facial recognition technology – whether by private actors or the state.[169] AI models intended to be neutral may inadvertently produce biased outcomes and discriminate.[170] AI may produce distorted pictures of individuals, whether a function of poor-quality or under-representative data sets used to train the algorithm[171] or aspects of human behavior that are not easily quantifiable.[172]

Then there are the technology's ripple effects on our democracy. For example, many traditional news outlets have suffered with the rise of the data-opolies.[173] Many websites, including traditional news outlets, rely on Google for advertising revenues[174] and traffic to their websites.[175] Ad revenues for newspapers declined 80% -- from $49 billion in 2006 to $9.7 billion in 2022; this decline was not offset by the rise in circulation revenue, which increased modestly from $10.5 billion to $11.6 billion.[176] Google and Facebook, while using the newspapers' content to attract individuals, have simultaneously siphoned off the newspapers' revenues.

As a result of Google's AI chatbot, news websites in 2025 were getting far less traffic from Google (and overall). To compete with ChatGPT and other AI models, Google introduced its *AI Overviews* tool in 2024 and then, in 2025, *AI Mode*, which "responds to user queries in a chatbot-

---

[168] Jeremy White, *How Strangers Got My Email Address From ChatGPT's Model*, N.Y. TIMES, Dec. 22, 2023, https://www.nytimes.com/interactive/2023/12/22/technology/openai-chatgpt-privacy-exploit.html.

[169] Daniel J. Solove, *Artificial Intelligence and Privacy*, 77 FLA. L. REV. 1, 60 (2025); UN AI Report, *supra* note, at 7 (noting how "Generative AI tools greatly reduce the difficulty of analysing and summarising massive corpuses of text data, including social media content," which in some contexts, "may supercharge existing forms of State surveillance that risk privacy violations on a large scale").

[170] Lara Mendes Bacalhau, Miguel Cachulo Pereira, & Joana Neves, *A Bibliometric Analysis of AI Bias in Marketing: Field Evolution and Future Research Agenda*, JOURNAL OF MARKETING ANALYTICS (2025), https://doi.org/10.1057/s41270-025-00379-6 (surveying research on how algorithms intended to be neutral may inadvertently produce biased outcomes, "such as in ad delivery systems where certain demographics are favored over others due to cost-effectiveness optimizations," how bias "can skew the effectiveness of marketing campaigns, leading to unequal representation and targeting of different consumer groups," and how biased AI systems "can perpetuate stereotypes and reinforce existing societal inequalities"); Tiwari Statement, *supra* note (noting how AI systems trained on biased data can perpetuate and amplify these biases, resulting in discriminatory outcomes); FTC 2024 Report, *supra* note, at 59 (noting that social media companies' AI "often make decisions about individuals without their knowledge, consent, or understanding and that consumers often have no recourse when it comes to biased or inaccurate data or decisions").

[171] OECD AI Report, *supra* note, at 3 (discussing how "[t]rustworthy AI requires trustworthy data").

[172] Solove, *supra* note, at 55-56.

[173] See STUCKE, BREAKING AWAY, *supra* note, at 94, 101-2, 240-41.

[174] *Id*. at 99-102.

[175] https://sparktoro.com/blog/who-sends-traffic-on-the-web-and-how-much-new-research-from-datos-sparktoro/#:~:text=The%20Largest%20Traffic%20Referrers%20on,sites%20initiated%20on%20Google.com.

[176] https://www.pewresearch.org/journalism/fact-sheet/newspapers/.

style conversation, with far fewer links."[177] The irony is that Google's AI relies on data from these third-party websites but does not direct users to these websites. As Nicholas Thompson, chief executive of *The Atlantic* magazine, said, "Google is shifting from being a search engine to an answer engine."[178] Now with even less traffic, newspapers have even less revenues, prompting more layoffs of journalists.[179] For example, *Business Insider* eliminated about 21% of its staff in 2025, "a move CEO Barbara Peng said was aimed at helping the publication 'endure extreme traffic drops outside of our control.'"[180] So, news organizations, which have already suffered under Google and Meta, will suffer even more as the walled gardens' AI paradoxically keeps users engaged with the news media's original content. Without a way to finance their journalism, more news outlets will likely pare back investigative journalism or shut down. More counties in the US will join the 200 counties in 2025 that were news deserts (i.e., communities "with limited access to the sort of credible and comprehensive news and information that feeds democracy at the grassroots level").[181]

As traditional journalism struggles, what will fill the void? For over a billion people (according to Meta's estimation[182]), Meta's highly personalized AI, which will be tailored for each user's context, interests, personality, culture, and "how they think about the world."[183] Meta's AI assistant, in tailoring the news to how that particular person thinks about the world, will likely reinforce, rather than challenge, that person's biases, and political and world-views. So, expect more echo chambers and more political division.[184] And it is not just Meta. The *New York Times* reported how other AI chatbots "are going down conspiratorial rabbit holes and endorsing wild, mystical belief systems." For some people, "conversations with the technology can deeply distort reality."[185]

Expect also foreign governments to use these AI models to sow discord. As Dr. Jessica Dawson of the US Army Cyber Institute observed, "What started as a way for businesses to connect directly with potential customers has transformed into a disinformation machine at a scale that autocratic

---

[177] Isabella Simonetti & Katherine Blunt, *News Sites Are Getting Crushed by Google's New AI Tools*, WALL ST. J., June 10, 2025, https://www.wsj.com/tech/ai/google-ai-news-publishers-7e687141?mod=hp_lista_pos2.

[178] *Id*.

[179] The number of people in the U.S. newspaper industry declined 70% between 2006 and 2021 to just 104,290 people. The number of newsroom employees more than halved, falling from 75,000 to less than 30,000. https://www.statista.com/statistics/626459/number-employees-newspaper-industry/.

[180] Simonetti & Blunt, *supra* note.

[181] UNC Hussman School of Journalism and Media, *Do You Live in a News Desert?*, https://www.usnewsdeserts.com.

[182] Meta Fourth Quarter 2024 Results Conference Call, *supra* note.

[183] *Id*.

[184] STUCKE, BREAKING AWAY, *supra* note, at 235-37.

[185] Hill, *supra* note.

governments of the past could only imagine."[186] Governments, such as Russia, China, and North Korea, can use AI to ramp up their "massive information warfare campaigns" with even more refined microtargeting and individual-level messaging to influence behavior, with even more "insidious dis/misinformation campaigns," including deepfakes.[187]

Moreover, politicians can use the data-opolies' AI models to propel themselves into power and maintain their control.[188] Facebook, as a former executive noted, "rewards outsider candidates who post inflammatory content that drives engagement," thereby "incentivizing and rewarding the worst kinds of political ugliness."[189]

Finally, there is the harm that social media can cause to children.[190] Judge Ryan D. Nelson of the US Court of Appeals for the Ninth Circuit said social media "might be actually worse than a carcinogen."[191] During an oral argument in a tech industry trade group's legal challenge to California's Protecting Our Kids from Social Media Addiction Act, which restricts children's access to platforms, the judge said, "'an entire generation" of children is facing addictive social media behaviors. 'There's a problem here.'"[192]

As we saw, Meta is racing to integrate its AI tools across its Instagram, WhatsApp, and Facebook platforms to increase engagement. How can Meta's AI chatbots increase engagement when its platforms are already addictive for many children? By engaging in graphic, sexually explicit conversations with children. As *The Wall Street Journal* reported, even when the users revealed their young age, Meta's AI personas, such as "Hottie Boy" and "Submissive Schoolgirl," would

---

[186] Jessica Dawson, *Microtargeting as Information Warfare*, 6 CYBER DEFENSE REVIEW 63, 64 (2021); WYNN-WILLIAMS, *supra* note, at 373 (raising a similar point about Meta).

[187] Dawson, *supra* note, at 63; see also UN AI Report, *supra* note, at 4 (noting that disinformation created with "generative AI may be used in ways that risk inciting targeted physical violence against specific individuals or groups, or destabilising societies in ways that risk inciting widespread, sporadic, or random violence (in relation to fictional terrorist attacks, coups, or electoral fraud") & 7 ("Broadly, the generation of false, defamatory information pertaining to specific individuals constitutes an attack on a person's honour and reputation. This may result from the intentional use of generative AI models to create and disseminate defamatory disinformation or the unintentional hallucinations of generative AI models."); Tiwari Statement, *supra* note.

[188] WYNN-WILLIAMS, *supra* note, at 250-251 (discussing how Philippines president weaponized Facebook's algorithm), 264-66 (discussing how the Trump campaign used Facebook to target voters with inflammatory misinformation and fundraising messages and for young women, white liberals who support Bernie Sanders, and Black voters with voter suppression campaigns), & 345-59 (how Meta's platforms were inflaming hate speech, violence, and ethnic tension in Myanmar).

[189] *Id*. at 251 & 252.

[190] FTC 2024 Report, *supra* note, at 63-64, 70-78 (quoting, inter alia, U.S. DEP'T OF HEALTH & HUM. SERVS., THE U.S. SURGEON GENERAL'S ADVISORY ON SOCIAL MEDIA AND YOUTH MENTAL HEALTH (May 23, 2023), at 9–10, https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf; Hunt Allcott et al., *Digital Addiction*, 112 AM. ECON. REV. 2424, 2424 (2022), https://pubs.aeaweb.org/doi/pdfplus/10.1257/aer.20210867).

[191] Isaiah Poritz, *Judge Likens Social Media to Tobacco in California Law Challenge*, BLOOMBERG (April 2, 2025), https://news.bloomberglaw.com/litigation/judge-likens-social-media-to-tobacco-in-california-law-challenge.

[192] *Id*.

steer conversations toward sexting (such as "a child who desires to be sexually dominated by an authority figure" or bondage fantasies) and "planning trysts to avoid parental detection."[193] Some Meta employees internally voiced concern: “the full mental health impacts of humans forging meaningful connections with fictional chatbots are still widely unknown. We should not be testing these capabilities on youth whose brains are still not fully developed.”[194] Nonetheless, Meta’s CEO Mark Zuckerberg “made multiple internal decisions to loosen the guardrails around the [AI] bots to make them as engaging as possible, including by providing an exemption to its ban on ‘explicit’ content as long as it was in the context of romantic role-playing.”[195]

E. Market Failure

Many Americans desire greater control over their privacy and data, including whether to be profiled (and if so, in what contexts), to be subject to behavioral advertising, and to have their data used to train AI models. In a 2021 survey, eighty-one percent preferred keeping their data private, "even if it means seeing less relevant ads," rather than seeing "relevant ads, even if companies are using [their] personal data to target them."[196] The concerns extend beyond behavioral advertising: 73% wished they had more control over their social media feeds, even if it meant seeing less engaging content, and 69% felt that using AI to personalize the news each user sees was dangerous.[197]

Market forces have not delivered. Individuals still lack control over their data and being profiled.[198] As the FTC found, the trend in the social media industry was not to give individuals any choice or even ask for their consent when using their personal information for AI purposes.[199] This includes “user and non-user data relating to activities both on and off of the [social media] platform (including data obtained or purchased from third parties).”[200]

When incentives are misaligned, more toxic competition is not the answer. To reorient competition – from toxic to beneficial -- policymakers must realign the market participants' incentives so that

---

[193] Jeff Horwitz, *Meta’s Chatbots Can Get Explicit*, WALL ST. J., Apr. 28, 2025, at A1 & A10.

[194] *Id*.

[195] *Id*.

[196] Greenberg Quinlan Rosner, Accountable Tech: Frequency Questionnaire, at 8 (Jan. 28-31, 2021), https://accountabletech.org/wp-content/uploads/Accountable-Tech-013121-FQ-Methodology.pdf.

[197] *Id*.

[198] UN AI Report, *supra* note, at 7 (noting that users’ “ability to provide informed consent to the collection, use and storage of their data for training of generative AI models may be compromised by the use of web-scraped datasets” and the data collected by generative AI models from users “may be aggregated and sold without users’ informed consent”).

[199] FTC 2024 Report, *supra* note, at 59.

[200] *Id*.

data is collected about us for our benefit. That requires giving individuals greater control over their data and its use. The next Part examines twenty recently enacted state privacy laws to see whether they can provide the guardrails needed to reorient competition from toxic to healthy.

II. How Do US Laws Currently Address Profiling and Behavioral Advertising?

As privacy scholar Daniel Solove observed, AI does not raise new privacy problems; it exasperates existing gaps in privacy protections and "demonstrates why certain long-overdue changes to privacy law are needed."[201] With no broad federal privacy law, states are filling the void. As of mid-2025, twenty states have enacted broad privacy protections for their residents.[202] Some of these states recognize privacy as a fundamental right.[203] Fundamental to this right of privacy is "the ability of individuals to control the use, including the sale, of their personal information."[204] Thus, starting with California in 2018, 20 states have given their residents greater control over their data, including accessing the personal data that a controller has collected about them, correcting inaccuracies in their data, deleting their data provided by or obtained about them, including personal data that a controller collected through third parties, and obtaining a copy of their data in a portable and readily usable format that allows them to transfer the data to another controller without hindrance.[205]

---

[201] Solove, *Artificial Intelligence & Privacy*, *supra* note, at 17.

[202] *California Consumer Privacy Act*, Cal. Civ. Code § 1798.140(z); *Colorado Privacy Act*, CO Revised Statutes § 6-1-1303(20); *Connecticut Consumer Data Privacy and Online Monitoring Act*, Conn. Gen. Stat. Ann. § 42-515(30); *Delaware Personal Data Privacy Act*, Del. Code Ann. tit. 6, § 12D-102(25); *Florida Digital Bill of Rights*, Fla. Stat. Ann. § 501.702; *Indiana Consumer Data Protection Act*, Ind. Code Ann. § 24-15-2-23; *Iowa Consumer Data Protection Act* (ICDPA), Iowa Code Title XVI, Subtit. 1, Ch. 715D et seq.; *Kentucky Consumer Data Protection Act*, Ky. Rev. Stat. Ann. § 367.3611(23); *Maryland Online Data Privacy Act*, Md. Code Ann., Com. Law § 14-4701(aa); *Minnesota Consumer Data Privacy Act*, Minn. Stat. Ann. § 325M.11; *Montana Consumer Data Privacy Act*, Mont. Code Ann. § 30-14-2802; *Nebraska Data Privacy Act*, Neb. Rev. Stat. Ann. § 87-1102; *New Hampshire Expectation of Privacy*, N.H. Rev. Stat. Ann. § 507-H:1; *New Jersey* N.J. Stat. Ann. § 56:8-166.4; *Oregon Control and Processing of Consumer Personal Data Act*, Or. Rev. Stat. Ann. § 646A.570; *Rhode Island Data Transparency and Privacy Protection Act*, R.I. Gen. Laws Ann. § 6-48.1-2; *Tennessee Information Protection Act*, Tenn. Code Ann. § 47-18-3302; *Texas Consumer Data Protection*, Tex. Bus. & Com. Code Ann. § 541.001(24); *Utah Consumer Privacy Act*, Utah Code §§ 13-61-101, et seq.; *Virginia Consumer Data Protection Act*, Va. Code § 59.1-571.

[203] *See, e.g.*, *California Consumer Privacy Act*, Cal. Civ. Code § 2 (noting how Californians voted to amended state constitution to include right to privacy as an "inalienable" right of all people); *Colorado Privacy Act*, CO Revised Statutes § § 6-1-1302(1)(A)(finding that the "people of Colorado regard their privacy as a fundamental right and an essential element of their individual freedom" and that state constitution "explicitly provides the right to privacy"); *Rhode Island Data Transparency and Privacy Protection Act* § 1 (finding right to privacy "a personal and fundamental right protected by the United States Constitution").

[204] *California Consumer Privacy Act*, Cal. Civ. Code § 2 (findings and declarations).

[205] See IAPP US State Privacy Legislation Tracker 2025, *supra* note. States are also enacting AI-focused consumer protection laws that go beyond the scope of this Article. Scott Kohler, *The Surge in State-Level Policymaking on AI*, *in* Technology Federalism: U.S. States at the Vanguard of AI Governance (Carnegie Endowment for International Peace 2025), https://www.jstor.org/stable/resrep67627.5.

For our purposes, we shall examine several privacy rights, namely, the resident's right to control (i) the processing of personal data for targeted advertising, (ii) profiling, and (iii) their sensitive personal data. All twenty states allow residents to opt out of the processing of some of their personal data for targeted advertising and the sale of personal data; in 18 states, residents can also opt out of some types of profiling.[206] (Iowa and Utah do not give their residents the right to opt out of profiling.[207])

Besides these opt-out rights, Minnesota residents have additional rights when they are profiled "in furtherance of decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer."[208] Minnesotans can

- question the result of the profiling,
- be informed of the reason that the profiling resulted in the decision,
- if feasible, be informed of what actions the consumer might have taken to secure a different decision and the actions that the consumer might take to secure a different decision in the future,
- review the consumer's personal data used in the profiling, and

---

[206] *California Consumer Privacy Act*, Cal. Civ. Code § 1798.140(z); *Colorado Privacy Act*, CO Revised Statutes § 6-1-1306(1)(a); *Connecticut Consumer Data Privacy and Online Monitoring Act*, Conn. Gen. Stat. Ann. § 42-518(a); *Delaware Personal Data Privacy Act*, Del. Code Ann. tit. 6, § 12D-104(a)(6); *Florida Digital Bill of Rights*, Fla. Stat. Ann. § 501.705(2)(e) (right to opt out of the processing of the personal data for purposes of targeted advertising; the sale of personal data; or profiling in furtherance of a decision that produces a legal or similarly significant effect concerning a consumer); *Indiana Consumer Data Protection Act*, Ind. Code Ann. § 24-15-3-1; *Iowa Consumer Data Protection Act* § 715D.3(1) (consumer has the right to opt out of the sale of personal data) & § 715D.4(6) ("If a controller sells a consumer's personal data to third parties or engages in targeted advertising, the controller shall clearly and conspicuously disclose such activity, as well as the manner in which a consumer may exercise the right to opt out of such activity"); *Kentucky Consumer Data Protection Act*, Ky. Rev. Stat. Ann. § 367; *Maryland Online Data Privacy Act*, Md. Code Ann., Com. Law § 14-4705(b); *Minnesota Consumer Data Privacy Act*, Minn. Stat. Ann. § 325O.05(1)(f); *Montana Consumer Data Privacy Act*, Mont. Code Ann. § 30-14-2808(1)(e); *Nebraska Data Privacy Act*, Neb. Rev. Stat. Ann. § 87-1107(2)(e); *New Hampshire Expectation of Privacy*, N.H. Rev. Stat. Ann. § 507-H:4(I)(E); N.J. Stat. Ann. §§ 56:8-166.6(b) & 56:8-166.10; *Oregon Control and Processing of Consumer Personal Data Act*, Or. Rev. Stat. Ann. § 646A.574(1)(d); *Rhode Island Data Transparency and Privacy Protection Act*, R.I. Gen. Laws Ann. § 6-48.1-5(e)(4); *Tennessee Information Protection Act*, Tenn. Code Ann. § 47-18-3203(2)(e); *Texas Consumer Data Protection*, Tex. Bus. & Com. Code Ann. § 541.051(b)(5); *Utah Consumer Privacy Act*, Utah Code § 13-61-201(4); *Virginia Consumer Data Protection Act*, Va. Code § 59.1-577(A)(5).

[207] Anokhy Desai, *Iowa Becomes Sixth US State to Enact Comprehensive Consumer Privacy Legislation*, IAPP, March 29, 2023, https://iapp.org/news/a/iowa-becomes-sixth-us-state-to-enact-comprehensive-consumer-privacy-legislation (noting that Iowa's law "notably does not provide the rights to correct personal data, not to be subject to fully automated decisions or to opt out of certain processing, such as for targeted advertising or profiling purposes. More specifically, while there is not an explicit right to opt out of targeted advertising in the law's consumer rights section, it does include a peculiar requirement for controllers that engage in targeted advertising to "clearly and conspicuously disclose such activity, as well as the manner in which a consumer may exercise the right to opt out of such activity"); https://dcp.utah.gov/wp-content/uploads/2024/01/UCPA-FOR-CONSUMERS.pdf; Taylor Kay Lively, *Utah Becomes Fourth US State to Enact Comprehensive Consumer Privacy Legislation*, IAPP, March 25, 2022, https://iapp.org/news/a/utah-becomes-fourth-state-to-enact-comprehensive-consumer-privacy-legislation/.

[208] *Minnesota Consumer Data Privacy Act*, Minn. Stat. Ann. § 325O.05 (1)(g).

- have the data corrected and the profiling decision reevaluated based upon the corrected data (if the decision is determined to have been based upon inaccurate personal data, considering the nature of the personal data and the purposes of the processing of the personal data).[209]

All 20 states also impose greater restrictions on "sensitive data," where firms cannot process sensitive data concerning a consumer without either (i) obtaining the consumer's consent[210] or (ii) giving the consumer the opportunity to opt out.[211]

Some states also seek to beef up their residents' consent. First, consent must be clear, unambiguous, affirmative action.[212] Second, consent must be "freely given, specific, informed."[213] Third, any purported consent obtained through dark patterns is void.[214] The state laws define dark

---

[209] *Id.*

[210] *Colorado Privacy Act*, CO Revised Statutes § 6-1-1308(7); *Connecticut Consumer Data Privacy and Online Monitoring Act,* Conn. Gen. Stat. Ann. § 42-520(a); *Delaware Personal Data Privacy Act*, Del. Code Ann. tit. 6, § 12D-106(a)(4); *Florida Digital Bill of Rights*, Fla. Stat. Ann. § 501.71(2)(d); *Indiana Consumer Data Protection Act*, Ind. Code Ann. § 24-15-4-1; *Kentucky Consumer Data Protection Act*, Ky. Rev. Stat. Ann. § 367.3617(1)(e); *Minnesota Consumer Data Privacy Act*, Minn. Stat. Ann. § 325O.07; *Montana Consumer Data Privacy Act*, Mont. Code Ann. § 30-14-2812(2)(b); *Nebraska Data Privacy Act*, Neb. Rev. Stat. Ann. § 87-1112(2)(d); *New Hampshire Expectation of Privacy*, N.H. Rev. Stat. Ann. § 507-H:6(I)(d); N.J. Stat. Ann. § 56:8-166.12; *Oregon Control and Processing of Consumer Personal Data Act*, Or. Rev. Stat. Ann. § 646A.578(2)(b); *Rhode Island Data Transparency and Privacy Protection Act*, R.I. Gen. Laws Ann. § 6-48.1-4(c); *Tennessee Information Protection Act*, Tenn. Code Ann. § 47-18-3204(a)(6); *Texas Consumer Data Protection*, Tex. Bus. & Com. Code Ann. § 541.101(b)(4); *Virginia Consumer Data Protection Act*, Va. Code § 59.1-578(A)(5).

[211] *California Consumer Privacy Act*, Cal. Civ. Code § 1798.121; *Iowa Consumer Data Protection Act*, Iowa Code Title XVI, Subtit. 1, Ch. 715D, § 715D.4(2); *Utah Consumer Privacy Act*, Utah Code §§ 13-61-302(3) Maryland has a slightly different approach to sensitive data, where a controller can collect or process sensitive data only when it is "strictly necessary to provide or maintain a specific product or service requested by the consumer." The controller may process personal data for another purpose if it obtains the consumer's consent. *Maryland Online Data Privacy Act*, Md. Code Ann., Com. Law § 14-4707(a)(1) & (8).

[212] *Colorado Privacy Act*, CO Revised Statutes § 6-1-1303(5); *Connecticut Consumer Data Privacy and Online Monitoring Act*, Conn. Gen. Stat. Ann. § 42-515(7); *Delaware Personal Data Privacy Act*, Del. Code Ann. tit. 6, § 12D-102(7); *Florida Digital Bill of Rights*, Fla. Stat. Ann. § 501.702(7); *Maryland Online Data Privacy Act*, Md. Code Ann., Com. Law § 14-4701(g); *Montana Consumer Data Privacy Act*, Mont. Code Ann. § 30-14-2802(5); NJ Stat. § 56:8-166.4; *Nebraska Data Privacy Act*, Neb. Rev. Stat. Ann. § 87-1102(6); *New Hampshire Expectation of Privacy*, N.H. Rev. Stat. Ann. § 507-H:1(VII); *Rhode Island Data Transparency and Privacy Protection Act*, R.I. Gen. Laws Ann. § 6-48.1-2(6); *Texas Consumer Data Protection*, Tex. Bus. & Com. Code Ann. § 541.001(6).

[213] *Colorado Privacy Act*, CO Revised Statutes § 6-1-1303(5); *Connecticut Consumer Data Privacy and Online Monitoring Act*, Conn. Gen. Stat. Ann. § 42-515(7); *Delaware Personal Data Privacy Act*, Del. Code Ann. tit. 6, § 12D-102(7); *Florida Digital Bill of Rights*, Fla. Stat. Ann. § 501.702(7); *Maryland Online Data Privacy Act*, Md. Code Ann., Com. Law § 14-4701(g); *Montana Consumer Data Privacy Act*, Mont. Code Ann. § 30-14-2802(5); NJ Stat. § 56:8-166.4; *Nebraska Data Privacy Act*, Neb. Rev. Stat. Ann. § 87-1102(6); *New Hampshire Expectation of Privacy*, N.H. Rev. Stat. Ann. § 507-H:1(VII); *Rhode Island Data Transparency and Privacy Protection Act*, R.I. Gen. Laws Ann. § 6-48.1-2(6); *Texas Consumer Data Protection*, Tex. Bus. & Com. Code Ann. § 541.001(6).

[214] *Colorado Privacy Act*, CO Revised Statutes § 6-1-1303(5); *Connecticut Consumer Data Privacy and Online Monitoring Act*, Conn. Gen. Stat. Ann. § 42-515(7); *Delaware Personal Data Privacy Act*, Del. Code Ann. tit. 6, §

patterns broadly as a "user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice," and include, in some states, "any practice the Federal Trade Commission refers to as a dark pattern."[215]

Some states whether through their privacy statute or other laws[216] also give broader rights for teenagers and those under the age of 13. For consumers 16 years of age and under, California, for example, requires "opt-in" consent for a business to sell or share the consumers' personal information.[217]

Because these privacy rights would be meaningless if businesses penalized consumers for exercising their rights, the state laws include anti-retaliation provisions. For example, under Tennessee's privacy law, a controller cannot "discriminate against a consumer for exercising the consumer rights" contained in Tennessee's privacy law, including "denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods and services to the consumer."[218] There are exceptions to the anti-retaliation provisions,[219] as well as exceptions to the exceptions of the anti-retaliation provision.[220]

Since many of these laws became effective in the past couple of years (or will become effective in 2026), it remains to be seen to what extent, if any, they will curb the AI-fueled profiling and behavioral advertising. Will they, for example, enable residents to opt out of Meta profiling them

12D-102(7); *Florida Digital Bill of Rights*, Fla. Stat. Ann. § 501.702(7); *Maryland Online Data Privacy Act*, Md. Code Ann., Com. Law § 14-4701(g); *Montana Consumer Data Privacy Act*, Mont. Code Ann. § 30-14-2802(5); NJ Stat. § 56:8-166.4; *Nebraska Data Privacy Act*, Neb. Rev. Stat. Ann. § 87-1102(6); *New Hampshire Expectation of Privacy*, N.H. Rev. Stat. Ann. § 507-H:1(VII); *Rhode Island Data Transparency and Privacy Protection Act*, R.I. Gen. Laws Ann. § 6-48.1-2(6); *Texas Consumer Data Protection*, Tex. Bus. & Com. Code Ann. § 541.001(6).

[215] *Connecticut Consumer Data Privacy and Online Monitoring Act,* Conn. Gen. Stat. Ann. § 42-515(14); *Rhode Island Data Transparency and Privacy Protection Act*, R.I. Gen. Laws Ann. § 6-48.1-2(11). For more on dark patterns see FTC, Press Release, FTC, ICPEN, GPEN Announce Results of Review of Use of Dark Patterns Affecting Subscription Services, Privacy (July 10, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/07/ftc-icpen-gpen-announce-results-review-use-dark-patterns-affecting-subscription-services-privacy

[216] *See, e.g.,* The California Age–Appropriate Design Code Act, Cal. Civ. Code § 1798.99.30; Florida Protection of Children in Online Spaces, Fla. Stat. Ann. § 501.1735; Maryland Age-Appropriate Design Code Act, Md. Code Ann., Com. Law § 14-4801.

[217] Cal. Civ. Code § 1798.120(c).

[218] Tenn. Code Ann. § 47–18–3204(a)(5).

[219] *See, e.g*., Tenn. Code Ann. § 47–18–3204(a)(5) (not prohibiting a "controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised the right to opt out pursuant to § 47–18–3203(a)(2)(F) or the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program").

[220] California, for example, has an exception to its anti-retaliation provision, whereby businesses may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale or sharing of personal information, or the retention of personal information. Businesses may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is reasonably related to the value provided to the business by the consumer's data. Cal. Civ. Code § 1798.125(a)(2) & (b)(1). Because of the potential abuse, California has an exception to the anti-retaliatory exception: "A business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature." *Id*. § 1798.125(b)(4).

and targeting them with behavioral ads? No, as the next Part discusses.

III. SHORTCOMINGS UNDER THE STATE PRIVACY LAWS

It is questionable whether the 20 state privacy laws will provide sufficient guardrails to reorient competition from the current race to the bottom to a race to the top. To see why, this Part considers first these laws' general limitations and then their specific shortcomings in opting out of profiling and behavioral advertising.

A. General Limitations

1. No Protection in Most States

As of mid-2025, 30 states and the District of Columbia did not have any comprehensive privacy laws. As Table A reflects, this represents approximately half of the US population:

Table A

States with privacy laws (in italics)	2024 Population (Estimate)	**% of Total Population**
Alabama	5,157,699	
Alaska	740,133	
Arizona	7,582,384	
Arkansas	3,088,354	
California	39,431,263	11.59%
Colorado	5,957,493	1.75%
Connecticut	3,675,069	1.08%
Delaware	1,051,917	0.31%
District of Columbia	702,250	
Florida	23,372,215	6.87%
Georgia	11,180,878	

Hawaii	1,446,146	
Idaho	2,001,619	
Illinois	12,710,158	
Indiana	6,924,275	2.04%
Iowa	3,241,488	0.95%
Kansas	2,970,606	
Kentucky	4,588,372	1.35%
Louisiana	4,597,740	
Maine	1,405,012	
Maryland	6,263,220	1.84%
Massachusetts	7,136,171	
Michigan	10,140,459	
Minnesota	5,793,151	1.70%
Mississippi	2,943,045	
Missouri	6,245,466	
Montana	1,137,233	0.33%
Nebraska	2,005,465	0.59%
Nevada	3,267,467	
New Hampshire	1,409,032	0.41%
New Jersey	9,500,851	2.79%
New Mexico	2,130,256	
New York	19,867,248	
North Carolina	11,046,024	
North Dakota	796,568	
Ohio	11,883,304	
Oklahoma	4,095,393	
Oregon	4,272,371	1.26%
Pennsylvania	13,078,751	
Rhode Island	1,112,308	0.33%
South	5,478,831	

Carolina		
South Dakota	924,669	
Tennessee	7,227,750	2.13%
Texas	31,290,831	9.20%
Utah	3,503,613	1.03%
Vermont	648,493	
Virginia	8,811,195	2.59%
Washington	7,958,180	
West Virginia	1,769,979	
Wisconsin	5,960,975	
Wyoming	587,618	
Total	340,110,988	50.15%

Residents in these 30 states must rely on the pre-existing patchwork of federal and state constitutional, common and statutory laws, which proved insufficient to curtail the harms of surveillance and behavioral advertising before the advent of AI. Moreover, two states with privacy laws, Iowa and Utah, do not allow residents to opt out of profiling. Thus, over half of the US population is vulnerable to AI-enhanced profiling and behavioral manipulation.

With an appropriate legal framework, state privacy protections can, at times, spill over to residents without privacy protection, especially when firms cannot easily and cost-effectively distinguish between residents protected under their state privacy laws and those who are not. However, that spillover is unlikely under the current privacy framework, as the following subparts discuss.

2. Default Bias

One feature common to the 20 state privacy laws is the default option–firms can continue to surveil their adult residents, use their non-sensitive personal data to profile them, and target them with behavioral ads. To protect their privacy, residents in these states must proactively visit the websites and apps and request that they not sell their data, profile them in certain contexts, or use specific personal data for behavioral advertising.

For spillover effects to work, enough residents in the 20 states must affirmatively opt out of behavioral advertising (and profiling in 18 states). How many residents will affirmatively opt? Likely very few, using the behavioral economics literature and Goggle monopolization case as

guides. Many people stick with the default option,[221] including decisions with important financial implications, like retirement savings.[222] As Google's internal behavioral economics team noted, "Inertia is the path of the least resistance. People tend to stick with the status quo, as it takes more effort to make changes."[223] For 18 years, Google used this default bias to help maintain its monopoly in search, entering into revenue sharing agreements to be the default search engine on key access portals, including Apple's Siri, Spotlight, and Safari browser.[224] In 2022 alone, Google paid Apple over $26 billion (or over $54 million per day) to be the default search engine.[225] Thus, if many residents stick with the privacy-unfriendly defaults, then profiling and behavioral advertising will continue as before.

One hopeful, countervailing sign was when Apple introduced new privacy features when updating its iOS 14.5 smartphone operating system. If an app "collects data about end users and shares it with other companies for purposes of tracking across apps and web sites," Apple requires that app developer to use Apple's AppTrackingTransparency framework.[226] Under this framework, Apple iPhone users are prompted when they first use that app to authorize cross-app and website tracking. As of April 2022, approximately 75 percent of Apple iPhone users opted not to allow tracking across other companies' apps and websites.[227]

However, unlike a default option, Apple's pop-up forced Apple users to decide on tracking before they could use the app. In contrast, under state privacy laws, residents must proactively go to each app's website and opt out of tracking. To see how time-consuming this task can be, consider how many firms track us. Two scholars from Princeton University examined the extent of online tracking on the top one million websites and found over 81,000 third-party trackers.[228] Not every website had trackers. On the one hand, websites that were less dependent on advertising revenues (such as governmental, nonprofit, and university websites) were far less likely to track users. On the other hand, websites that lacked external funding sources and relied primarily on advertising revenue, such as news sites, had the most trackers on their websites. While the 2016 Princeton study identified many third-party trackers (over 81,000), some track us far more extensively than

---

[221] Default (option/setting), https://www.behavioraleconomics.com/resources/mini-encyclopedia-of-be/default-optionsetting/.

[222] https://www.nber.org/papers/w8651; Hu, J. (2025). What Behavioral Principles Should Be Used to Design a Pension Scheme: Insights from Status Quo Bias and Hyperbolic Discounting. Advances in Economics, Management and Political Sciences,133,82-97.

[223] United States v. Google LLC, 747 F. Supp. 3d 1, 45 (D.D.C. 2024).

[224] *Id*. at 89-90.

[225] *Id*. at 32.

[226] Apple, App Tracking Transparency, https://developer.apple.com/documentation/apptrackingtransparency

[227] https://www-statista-com.utk.idm.oclc.org/statistics/1234634/app-tracking-transparency-opt-in-rate-worldwide/#statisticContainer

[228] Steven Engelhardt & 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.

others. Many companies track us only on a few websites. Of these 81,000 third-party trackers, only 123 were tracking us on more than 10,000 websites. Only four companies—Google, Facebook, Twitter, and AdNexus—had trackers on more than 100,000 websites.

Residents should not have to ask hundreds of thousands of websites and apps not to share their data with Google, Meta, or any other third party. A solution like Apple's would help consumers protect their privacy. One problem with the opt-out approach is that it does not scale. Suppose the average internet user visits 130 websites per day.[229] Suppose it takes users, for each website, one minute to opt out of targeted advertising, profiling, and the sale of their data. That would take 2 hours and 10 minutes to opt out of the first 130 websites. That would consume more time than what Americans spend on average on household activities (1.92 hours in 2023), eating and drinking (1.20 hours), or caring for and helping household children and parents (1.40 hours).[230] Few, if any, would have the time and patience to undertake this tedious task. If the website adds a bit more friction to opting out (such as requiring one to navigate several links), even fewer people will likely opt out.[231]

Recognizing this, some states allow their residents to opt out of profiling and targeted advertising through browser extensions or other technological means.[232] Consumers may designate authorized agents by way of technologies, including "an Internet link or a browser setting, browser extension or global device setting, indicating such consumer's intent to opt out of such processing."[233]

However, this opt-out technology allows firms "to accurately determine whether the consumer is a resident of [the state that affords this technological solution] and whether the consumer has made a legitimate request to opt out of any sale of such consumer's personal data or targeted advertising."[234] For spillover effects to work, firms cannot effectively discriminate between residents of states with privacy protections and those without such protections. Consequently, in delineating the user's location and residence, companies can deny opt-out requests from residents in states without comprehensive privacy laws.

---

[229] https://bloggingwizard.com/website-statistics/

[230] U.S. Bureau of Labor Statistics, American Time Use Survey, https://www.bls.gov/tus/latest-numbers.htm.

[231] *Google*, 747 F. Supp. 3d at 46–47 (noting how increased friction discourages users from switching from default, quoting Google's Behavioral Economics Team that a "[s]eemingly small friction points in user experiences can have a dramatically disproportionate effect on whether people drop or stick"); ("[Y]ou want to think about each step, as small as it might be, and see if there is a way to eliminate it, delay it, simplify it, default it."); ("[O]f the tiny fraction of end users who try to change the default, many will become frustrated and simply leave the default as originally set[.]").

[232] *See, e.g.*, *Connecticut Consumer Data Privacy and Online Monitoring Act*, Conn. Gen. Stat. Ann. § 42-519 (allowing consumers to "designate another person to serve as the consumer's authorized agent, and act on such consumer's behalf, to opt out of the processing of such consumer's personal data" for one or more of specified purposes, including targeted advertising and profiling).

[233] *Id.*

[234] *Id.* at § 42-520(e)(1)(A)(ii)(V).

B. Laws' Specific Shortcomings on Profiling and Behavioral Advertising

Let us turn to the states where residents can opt out of behavioral advertising, profiling, and the sale of their data. Will these residents who opted out be protected from AI-profiling and emotional advertising? Not necessarily, as the following subparts address.

1. Caveats to the Definition of Personal Information

In the 18 states where residents can opt out of profiling, and in the 20 states where residents can opt out of behavioral advertising, the right only protects "personal information." On the surface, the statutory right appears broad, as the laws define personal information or data broadly, such as "information that is linked or reasonably linkable to an identified or identifiable natural person."[235] California even includes households in its definition of personal information.[236] But the laws exclude from their definition of personal information, data that is: (i) publicly available,[237] (ii) aggregated, or (iii) de-identified.[238] This means that even if residents opt out, companies can continue using these three categories of personal data for targeted advertising and profiling.

Ordinarily, these exceptions should not be an issue. After all, one may not expect privacy in one's publicly available data. Nor should one be concerned with "data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to that individual."[239]

But with AI, these three statutory exceptions potentially create a significant loophole for advertisers and data-opolies.

To see why, suppose a thirty-year-old article published in the print edition of *The Wall Street Journal* reveals incriminating but misleading information about an individual. *The Wall Street Journal*'s owner, News Corp., has agreed to license its news publications, including archives, to OpenAI to help train its foundation models, such as ChatGPT.[240] Now, suppose that ChatGPT,

---

[235] *See, e.g.*, Tenn. Code Ann. § 47-18-3201(17); Conn. Gen. Stat. Ann. § 42-515(18).

[236] Cal. Civ. Code § 1798.140(v) (defining "personal information" as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household").

[237] *See, e.g.*, Conn. Gen. Stat. Ann. §§ 42-515(18) & (25) (excluding from its definition of personal information "publicly available information," which "means information that (A) is lawfully made available through federal, state or municipal government records or widely distributed media, and (B) a controller has a reasonable basis to believe a consumer has lawfully made available to the general public").

[238] *See, e.g.*, Tenn. Code Ann. § 47-18-3201(17) (excluding "[d]e-identified or aggregate consumer information" from its definition of personal information); Conn. Gen. Stat. Ann. § 42-515(18) (excluding de-identified data or publicly available information from its definition of personal information).

[239] Tenn. Code Ann. § 47-18-3201(11) (defining de-identified data).

[240] Alexandra Bruell et al., *OpenAI, WSJ Owner News Corp Strike Content Deal Valued at Over $250 Million*, WALL ST. J., May 22, 2024, https://www.wsj.com/business/media/openai-news-corp-strike-deal-23f186ba.

trained on that article, along with other *Journal* articles, reveals misleading information when one searches that individual's name on ChatGPT. Does one have the right to correct it? The answer depends in part on whether that data is deemed "publicly available information." Yes, in some states,[241] but not in others.[242] States define publicly available data differently, and what constitutes publicly available information "may not correlate to the lay definition understood by many businesses and individuals."[243] Not surprisingly, other jurisdictions are questioning the binary distinctions between "personal data" and "non-personal data," as "big data blurs these distinctions, making it arduous to pre-determine the nature of data collected."[244]

Second, AI can collect scattered pieces of publicly available data to create a highly revealing mosaic of a person's life. This was a concern for the US Supreme Court regarding rap sheets and for European courts regarding the ease with which Google's search engine can compile information about individuals.

In *DOJ v. Reporters Committee for Freedom of the Press*, reporters sought, under the Freedom of Information Act, the FBI's criminal identification records, also known as "rap sheets," for four members of the Medico family, who ran a company that obtained defense contracts through improper arrangements with a corrupt Congressman.[245] The rap sheets contained descriptive information (e.g., date of birth) and history of arrests, charges, convictions, and incarcerations of the subject.[246] The issue before the Court was whether the disclosure of an individual's rap sheet would "reasonably be expected" to constitute an "unwarranted invasion of personal privacy" to exempt its production under the Freedom of Information Act. Much of the information was a matter of public record.[247] But the fact that "an event is not wholly 'private' does not mean that an individual has no interest in limiting disclosure or dissemination of the information."[248] The Supreme Court distinguished the difference in one's expectation of privacy over isolated scattered bits of data which would be time-consuming and expensive to collate and all of this information centralized in one computerized rap sheet database: "Plainly there is a vast difference between the

---

[241] Conn. Gen. Stat. Ann. § 42-515(33) (defining "publicly available information" as "information that (A) is lawfully made available through federal, state or municipal government records or widely distributed media, and (B) a controller has a reasonable basis to believe a consumer has lawfully made available to the general public").

[242] CO Revised Statutes § 6-1-1303(17)(b) (defining "publicly available information" as "information that is lawfully made available from federal, state, or local government records and information that a controller has a reasonable basis to believe the consumer has lawfully made available to the general public").

[243] David A. Zetoony, *What is 'Publicly Available Information' under the State Privacy Laws?*, NAT'L LAW REV., Sept. 13, 2023, https://natlawreview.com/article/what-publicly-available-information-under-state-privacy-laws.

[244] The intersection between competition and data privacy-Note by Italy, DAF/COMP/WD(2024)35 (22 May 2024).

[245] 489 U.S. 749, 757 (1989).

[246] *Id*. at 752.

[247] *Id*. at 753 (noting that "[a]rrests, indictments, convictions, and sentences are public events that are usually documented in court records").

[248] *Id*. at 770 (internal citation omitted).

public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."[249]

Fast forward 25 years to the European case, *Google Spain Inc. v. González*, Case C-131/12 (13 May 2014). There, a Spanish citizen lodged a complaint with Spain's privacy agency against a Spanish newspaper and Google. The citizen complained that the real-estate auction notice in the newspaper infringed his privacy rights because the attachment proceedings against him for the recovery of social security debts had been fully resolved for many years and, therefore, the reference to these attachment proceedings was entirely irrelevant. In searching the complainant's name on Google, however, one would obtain links to two pages of *La Vanguardia*'s newspaper, of 19 January and 9 March 1998, on which an announcement mentioning the complainant's name appeared for this real-estate auction. The complainant requested, first, that the newspaper remove or alter these two pages so that the personal data relating to him no longer appeared and, second, that Google removes the personal data relating to him so that these newspaper articles no longer appeared in the search results. The Spanish Data Protection Agency rejected the citizen's complaint against the newspaper. However, it upheld his complaint against Google, ordering Google to remove personal data relating to Mr. González from its index and to prevent future access to the data. Google appealed, and Spain's Audiencia Nacional (National High Court) referred several questions to the European Court of Justice for a preliminary ruling regarding the interpretation of the European Data Directive [95/46] on the right to privacy. One issue was an individual's right to privacy in truthful information published in a newspaper. Although anyone could still find that article online, for the European Court of Justice, like the Supreme Court in *Reporters Committee*, there was a vast difference in information publicly available both online and offline, and the inclusion of that publicly available information in the list of search results for that person's name. Google made access to that publicly available information "appreciably easier for any internet user making a search in respect of the person concerned and may play a decisive role in the dissemination of that information," and thus, the Google search "is liable to constitute a more significant interference with the data subject's fundamental right to privacy than the publication on the web page."

Now consider an AI model trained on data indexed for a search engine plus other publicly available data. There is a difference between Googling one's name, which can produce numerous links that require more time and effort to review than asking Google's AI model about that person. Unlike Google's search engine, which provides web page links that reference the individual, AI synthesizes the data from a greater reservoir of data. One conservative activist, for example, sued Meta for defamation when its foundation model falsely stated that he participated in the January

[249] *Id*. at 764.

6, 2021 Capitol riot and was linked to QAnon.[250] But suppose those statements were true. Finding that information with a search engine would likely take longer than the seconds it takes for an AI model to reveal these unsavory acts.

As the Supreme Court noted in *Reporters Committee*, in an organized society, there are few facts that are not at one time or another divulged to another. Nonetheless, the Court, in that case, emphasized the importance of one's ability to control information concerning oneself. That privacy right should not cease if the information is "publicly available," as defined under the state privacy laws. That is especially true of some obscure facts that are now given prominence by Siri or other AI assistants, which were previously buried online.

A third issue is the ease with which AI can infer personal details from otherwise innocuous, publicly available information.[251] How wealthy are you? Do you use cocaine? Ordinarily, one would be uncomfortable answering these questions. However, AI models can infer this information from publicly available data. Even seemingly benign bits of information—such as what we "Like" on Facebook—can tell Facebook and advertisers a lot about us. Using one's Likes, computer scientists at one university, with their algorithm, could estimate a Facebook user's sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender.[252] When you "Like" something using Facebook's tools, that, by itself, does not reveal any "sensitive personal information" under the state statutes. However, with enough seemingly benign "Likes," one can gain revealing, sensitive insights about that individual. Indeed, in 2016, Facebook sought a patent to infer your socio-economic class based on your "likes" and other public information.[253]

As Professor Solove observed, "Privacy legislation tends to concentrate on the actual gathering of data rather than on the creation of data through inferential processes."[254] As a result, "many privacy laws grant individuals rights to amend their data or consent to its collection," Solove noted, but "those laws seldom provide means to challenge or rectify inferences drawn from individuals'

---

[250] Sarah Nassauer & Jacob Gershman, *Activist Robby Starbuck Sues Meta Over AI Answers About Him*, WALL ST. J., Apr. 29, 2025, https://www.wsj.com/tech/ai/activist-robby-starbuck-sues-meta-over-ai-answers-about-him-9eba5d8a.

[251] Solove, *supra* note, at 36-37.

[252] Michal Kosinski, David Stillwell, & Thore Graepel, *Private Traits and Attributes Are Predictable from Digital Records of Human Behavior*, 110 PROC. NAT'L ACAD. SCI. 5802 (2013), https://doi.org/10.1073/ pnas.121 8772 110.

[253] Socioeconomic group classification based on user features, US Patent No. US-10607154-B2, https://ppubs.uspto.gov/api/pdf/downloadPdf/10607154?requestToken=eyJzdWIiOiIwZGQwM2FmMi0wZGZkLTRlZGItODdiNS0zZTg0ZDJmNTA5YWQiLCJ2ZXIiOiJiY2YzNDk1ZS04MGRiLTRiOWQtOWQ5OC1iNDA0MWIwNDFlMGUiLCJleHAiOjB9, Lily Li, *Facebook, Patents, and Privacy*, 37 GPSOLO 18, 20 (September/October 2020), https://www.jstor.org/stable/10.2307/27044794.

[254] Solove, *supra* note, at 38; see also Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 NW. U. L. REV. 357 (2022), https://scholarlycommons.law.northwestern.edu/nulr/vol117/iss2/1.

data."[255] Thus, "[t]he power of AI to make inferences renders many provisions and goals of current privacy law moot."[256]

As we saw in Part II, the Minnesota Consumer Data Privacy Act provides its residents with broader rights regarding AI profiling. Nonetheless, even this law falls short in terms of inferences. First, the rights do not apply to inferences made from "publicly available information."[257] Second, the law emphasizes the residents' right to review their *personal data* used in profiling and have that *data* corrected, as well as the profiling decision reevaluated based on the corrected *data* (rather than the inferences made from that data).[258] Moreover, this right is limited, as the next subpart examines, to only when a "consumer's personal data is profiled in furtherance of decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer."[259]

Therefore, even under state privacy laws, AI foundation models, trained on seemingly innocuous publicly available data, may nonetheless make inferences about an individual's preferences, characteristics, psychological traits, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes. Even when the inferences reveal sensitive personal information, if the input is "publicly available," as defined under the state law, then companies can use the data and inferences for profiling and behavioral advertising.

A fourth concern is how AI can transform publicly available data into uses that individuals neither contemplated nor agreed to. Consider Clearview AI, which was sued for scraping millions of websites to amass a data set of 3 billion facial images without obtaining the consent of individuals in the images or the companies whose websites were scraped.[260] If you or someone else posted a photo of you on Facebook, Instagram, or LinkedIn, then "your social media profile picture, vacation snapshots, or family photos may well be part of a facial recognition dragnet that's been tested or used by law enforcement agencies across the country."[261] New York City's police department, for example, was among the 1,803 publicly funded agencies that used Clearview AI facial recognition software.[262] One NY court noted how "many people fear that employment of such software will erode First Amendment rights by permitting unfriendly officials to identify and

---

[255] Solove, *supra* note, at 39.

[256] *Id*.

[257] Minn. Stat. Ann. § 325O.02(p) (personal data excludes publicly available information, which is "information that (1) is lawfully made available from federal, state, or local government records or widely distributed media, or (2) a controller has a reasonable basis to believe has lawfully been made available to the general public").

[258] *Id.* § 325O.05(1)(g).

[259] *Id*.

[260] GAO, Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses GAO-20-522 (July 13, 2020).

[261] https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition

[262] *Id*.

take action against those who demonstrate against government policies. That concern is especially pronounced given the ubiquity of security cameras in many big-city areas."[263] But ultimately, the court left these concerns for the state legislature to resolve. So, as this case reflects, "AI dramatically escalates scraping because AI creates incentives to scrape more frequently and extensively,"[264] especially when the scraped data is publicly available, transformed into profitable uses, and falls outside the state privacy laws.

A fifth concern is how AI might easily re-identify individuals to the de-identified data based on other publicly available data. The risk of re-identification existed before the advent of generative AI. But foundation models increase the risk of re-identifying individuals using publicly available information.[265] The state privacy laws do not apply to de-identified data, but the laws, like the Connecticut Consumer Data Privacy and Online Monitoring Act, require controllers in possession of de-identified data to take "reasonable measures to ensure that the data cannot be associated with an individual."[266] In collecting and using aggregated and de-identified data to train the foundation model, the company may believe that the privacy laws do not apply. But the foundation model, unbeknownst to the controller, may be able to reidentify the data. Nor will the foundation model necessarily alert the controller when it has linked the de-identified data to particular individuals. As a result, it can be challenging for the controller or state attorney general to determine if and when AI can reasonably link the data to an identified or identifiable natural person.

2. Other Gaps in Profiling

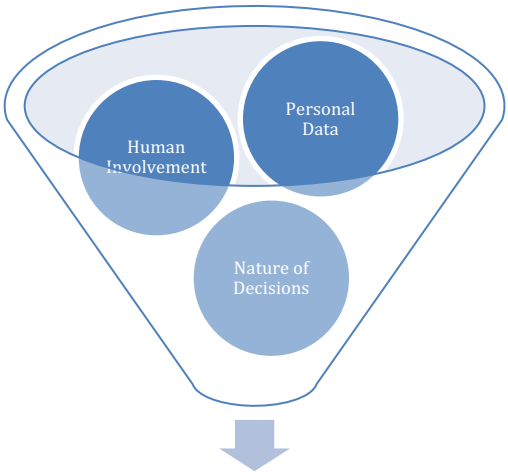
In the 18 states where residents can opt out of profiling, there is a funnel effect that diminishes the individual's right:

[263] People v. Reyes, 69 Misc. 3d 963, 133 N.Y.S.3d 433 (N.Y. Sup. Ct. 2020).

[264] Solove, *supra* note, at 28.

[265] Katerina Megas, National Institute of Standards and Technology, Managing Cybersecurity and Privacy Risks in the Age of Artificial Intelligence: Launching a New Program at NIST, Cybersecurity Insights (Sept. 19, 2024) (noting how AI creates new re-identification risks, "not only because of its analytic power across disparate datasets, but also because of potential data leakage from model training").

[266] Conn. Gen. Stat. Ann. § 42-523(a); see also Cal. Civ. Code § 1798.140(m) (defining "deidentified" as "information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer," provided that, inter alia, "the business that possesses the information [] takes reasonable measures to ensure that the information cannot be associated with a consumer or household").



First, as we have seen, the state laws only apply to personal data, which excludes publicly available data. However, even if companies used non-publicly available "personal data" to train their AI to profile individuals, two other statutory qualifiers further diminish the opt-out right: human involvement in the profiling and the nature of the decisions made during the profiling.

a. Human Involvement

As the FTC found, most of the leading social media companies had some level of human review or involvement in monitoring, testing, and reviewing the decisions made by AI.[267] But this human involvement did not assuage the FTC's concerns: some of the social media companies "provided more specifics than others (with some offering vague descriptions of the role of human reviewers), and the scope, level of involvement, and overall effects of human reviewers on automated processes differed."[268] Even when humans reviewed the AI, it was unclear "whether human reviewers were empowered to meaningfully change or alter flawed models."[269] The social media companies "did not specify the qualifications of reviewers, whether reviewers were employees or external to the Company, and whether reviewers represented diverse backgrounds, viewpoints, and perspectives."[270]

AI-generated profiling, conducted without human involvement, raises additional concerns,

[267] FTC 2024 Report, *supra* note, at 68.

[268] *Id.*

[269] *Id.* at 69.

[270] *Id.*

including hallucinations and inaccurate profiles. However, the harms identified in Part I do not disappear if humans were somehow involved in the profiling. As Part I discusses, the harm from profiling stems from the underlying business model and the incentives it creates to predict and manipulate behavior—not whether humans were involved. Nonetheless, in all but six states, residents lose their right to opt out of profiling if humans had any involvement, no matter how minor. (Europe's GDPR suffers from this same limitation.[271])

To see why, let us first examine how the states define profiling. Thirteen states define "profiling" broadly and similarly as any form of automated processing performed on personal data "to evaluate, analyze or predict personal aspects" related to an identified or identifiable individual's "economic situation, health, personal preferences, interests, reliability, behavior, location, or movements."[272] Five states, however, define profiling more narrowly as "*solely* automated processing."[273] So, suppose any human involvement, no matter how little, in the processing of personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual. In that case, it is not "profiling" under these five state laws.

---

[271] The GDPR defines profiling broadly. Council Regulation 2016/679, art. 4(4), 2016 O.J. (L 119) 46 (defining the term as "*any* form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular, to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements") (emphasis added). But the GDPR then limits the substantive privacy right to decisions "based *solely* on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." Council Regulation 2016/679, art. 22(1), 2016 O.J. (L 119) 46 (emphasis added).

[272] *Connecticut Consumer Data Privacy and Online Monitoring Act*, Conn. Gen. Stat. Ann. § 42-515(30); *Colorado Privacy Act*, CO Revised Statutes § 6-1-1303(20) (same); *Delaware Personal Data Privacy Act*, Del. Code Ann. tit. 6, § 12D-102(25) (same); *Kentucky Consumer Data Protection Act*, Ky. Rev. Stat. Ann. § 367.3611(23) (same); *Minnesota Consumer Data Privacy Act*, Minn. Stat. Ann. § 325M.11(s) (same); *Montana Consumer Data Privacy Act*, Mont. Code Ann. § 30-14-2802(19) (same); *New Hampshire Expectation of Privacy*, N.H. Rev. Stat. Ann. § 507-H:1 (XXIII) (same); N.J. Stat. Ann. § 56:8-166.4 (same); *Rhode Island Data Transparency and Privacy Protection Act*, R.I. Gen. Laws Ann. § 6-48.1-2(21) (same); *Virginia Consumer Data Protection Act*, Va. Code § 59.1-571 (same); see also *California Consumer Privacy Act*, Cal. Civ. Code § 1798.140(z) (defining "profiling" as any form of automated processing of personal information, as further defined by regulations pursuant to paragraph (15) of subdivision (a) of Section 1798.185, to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements"); *Maryland Online Data Privacy Act*, Md. Code Ann., Com. Law § 14-4701(aa) (defining "profiling" as "any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable consumer's economic situation, health, *demographic characteristics*, personal preferences, interests, reliability, behavior, location, or movements"); *Oregon Control and Processing of Consumer Personal Data Act*, Or. Rev. Stat. Ann. § 646A.570(16) (defining "profiling" as "an automated processing of personal data for the purpose of evaluating, analyzing or predicting an identified or identifiable consumer's economic *circumstances*, health, personal preferences, interests, reliability, behavior, location or movements").

[273] *Florida Digital Bill of Rights*, Fla. Stat. Ann. § 501.702(25) ("any form of *solely* automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements"); *Indiana Consumer Data Protection Act*, Ind. Code Ann. § 24-15-2-23 (same); *Nebraska Data Privacy Act*, Neb. Rev. Stat. Ann. § 87-1102(25) (same); *Tennessee Information Protection Act*, Tenn. Code Ann. § 47-18-3302 (same); *Texas Consumer Data Protection*, Tex. Bus. & Com. Code Ann. § 541.001(24) (same).

Of the remaining 13 states with a broad statutory definition of profiling, residents in six states cannot opt out of profiling where a human was involved in the decision. This is because the opt-out right applies only to the processing of personal data for purposes of profiling "in furtherance of *solely* automated decisions that produce legal or similarly significant effects concerning the consumer."[274] In effect, the opt-out right in these six states is similar to that in the five states, which limit their definition of profiling to "*solely* automated processing."[275] This means that companies in 11 of the 18 states can nullify residents' right to opt out of profiling by involving some human element in the processing, regardless of its extent.

In California, the right to opt out of profiling, as of mid-2025, was still subject to regulatory notice and comment. Consequently, as of mid-2025, residents in only six states – Colorado, Kentucky, Minnesota, New Jersey, Oregon, and Virginia, which collectively constitute 11.5% of the US population – could opt out of profiling where a human was involved – in either the profiling or in furtherance of decisions "that produce legal or similarly significant effects" concerning the consumer.[276]

However, as the next subpart discusses, even residents of these six states cannot generally opt out of profiling.

b. Nature of Decisions

No state allows its residents to opt out of profiling generally. California, as noted, is still in the process of promulgating regulations. The remaining 17 states limit the statutory right to opt out of profiling to "decisions that produce legal or similarly significant effects" concerning the consumer. The states generally define that term as

- *decisions* [in some states - made by the controller]
- *that result in the provision or denial* [in some states - by the controller] of
    - financial or lending services,
    - housing,
    - insurance,

[274] *Connecticut Consumer Data Privacy and Online Monitoring Act*, Conn. Gen. Stat. Ann. § 42-518(a) (italics added); see also *Delaware Personal Data Privacy Act*, Del. Code Ann. tit. 6, § 12D-104(a)(6) (same); *Maryland Online Data Privacy Act*, Md. Code Ann., Com. Law § 14-4705(b) (same); *Montana Consumer Data Privacy Act*, Mont. Code Ann. § 30-14-2808(1)(e) (same); *New Hampshire Expectation of Privacy*, N.H. Rev. Stat. Ann. § 507-H:4(I)(E) (same); *Rhode Island Data Transparency and Privacy Protection Act*, R.I. Gen. Laws Ann. § 6-48.1-5(e)(4) (same).

[275] Compare, for example, Tenn. Code Ann. § 47-18-3203(a)(2)(E)(iii) with Conn. Gen. Stat. Ann. §§ 42-515 & 42-518.

[276] *Colorado Privacy Act*, CO Revised Statutes § 6-1-1306(1)(a); *Kentucky Consumer Data Protection Act*, Ky. Rev. Stat. Ann. § 367; *Minnesota Consumer Data Privacy Act*, Minn. Stat. Ann. § 325O.05(1)(f); N.J. Stat. Ann. §§ 56:8-166.6(b) & 56:8-166.10; *Oregon Control and Processing of Consumer Personal Data Act*, Or. Rev. Stat. Ann. § 646A.574(1)(d); *Virginia Consumer Data Protection Act*, Va. Code § 59.1-577(A)(5).

- education enrollment or opportunity,
- criminal justice,
- employment opportunities,
- healthcare services, or
- access to basic necessities, such as food and water[277] [or in some states,

[277] Tenn. Code Ann. § 47-18-3201(10); see also *Connecticut Consumer Data Privacy and Online Monitoring Act*, Conn. Gen. Stat. Ann. § 42-515(15) (defining term as "decisions made by the controller that result in the provision or denial by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services or access to essential goods or services"); *Delaware Personal Data Privacy Act*, Del. Code Ann. tit. 6, § 12D-102(13) (defining term as "decisions made by the controller that result in the provision or denial by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services"); *Florida Digital Bill of Rights*, Fla. Stat. Ann. § 501.702(12) (defining term as "a decision made by a controller which results in the provision or denial by the controller of any of the following: (a) Financial and lending services. (b) Housing, insurance, or health care services. (c) Education enrollment. (d) Employment opportunities. (e) Criminal justice. (f) Access to basic necessities, such as food and water."); *Indiana Consumer Data Protection Act*, Ind. Code Ann. § 24-15-2-11 (defining term as "a decision made by a controller that results in the provision or denial by the controller of: (1) financial and lending services; (2) housing; (3) insurance; (4) education enrollment; (5) criminal justice; (6) employment opportunities; (7) health care services; or (8) access to basic necessities, such as food and water"); *Kentucky Consumer Data Protection Act*, Ky. Rev. Stat. Ann. § 367.3611(10) (defining term as "a decision made by a controller that results in the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities like food and water"); *Maryland Online Data Privacy Act*, Md. Code Ann., Com. Law § 14-4701(o) (defining term as "decisions that result in the provision or denial of: (1) Financial or lending services; (2) Housing; (3) Education enrollment or opportunity; (4) Criminal justice; (5) Employment opportunities; (6) Health care services; or (7) Access to essential goods or services"); *Minnesota Consumer Data Privacy Act*, Minn. Stat. Ann. § 325M.11(i) (defining term as "decisions made by the controller that result in the provision or denial by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services, or access to essential goods or services"); *Montana Consumer Data Privacy Act*, Mont. Code Ann. § 30-14-2802(10) (defining term as "decisions made by the controller that result in the provision or denial by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services, or access to necessities such as food and water"); *Nebraska Data Privacy Act*, Neb. Rev. Stat. Ann. § 87-1102(11) (defining term as "a decision made by the controller that results in the provision or denial by the controller of: (a) Financial and lending services; (b) Housing, insurance, or health care services; (c) Education enrollment; (d) Employment opportunities; (e) Criminal justice; or (f) Access to basic necessities, such as food and water"); *New Hampshire Expectation of Privacy*, N.H. Rev. Stat. Ann. § 507-H:1(XIII) (defining term as "decisions made by the controller that result in the provision or denial by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services or access to essential goods or services"); N.J. Stat. Ann. § 56:8-166.4 (defining term as "decisions that result in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services, or access to essential goods and services"); *Oregon Control and Processing of Consumer Personal Data Act*, Or. Rev. Stat. Ann. § 646A.570(10) (defining term as "decisions that result in providing or denying financial or lending services, housing, insurance, enrollment in education or educational opportunity, criminal justice, employment opportunities, health care services or access to essential goods and services. "profiling" as "an automated processing of personal data for the purpose of evaluating, analyzing or predicting an identified or identifiable consumer's economic circumstances, health, personal preferences, interests, reliability, behavior, location or movements"); *Rhode Island Data Transparency and Privacy Protection Act*, R.I. Gen. Laws Ann. § 6-48.1-2(12) (defining term as "decisions made by the controller that result in the provision or denial by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services or access to essential goods or services"); *Texas Consumer Data Protection*, Tex. Bus. & Com. Code Ann. § 541.001(11) (defining term as "a

"access to essential goods or services"].[278]

Profiling to maximize engagement, manipulate behavior, and increase behavioral advertising revenues do not fall within these statutory categories. As a result, gambling apps can continue to profile users to encourage them to gamble more.[279] The profiling opt-out right will not materially impact the data-opolies' revenues, since Meta and Google can continue to profile users to sustain their attention and click ads. But these laws may ensnare other companies, such as Yum! Brands, if the state enforcers and courts consider its fast-food and drinks as "access to basic necessities."

Consequently, these 17 laws will not place meaningful guardrails to curb the AI-driven profiling discussed in Part I. Indeed, residents in these states may have a false sense of security in thinking they have opted out of being profiled when they have not.

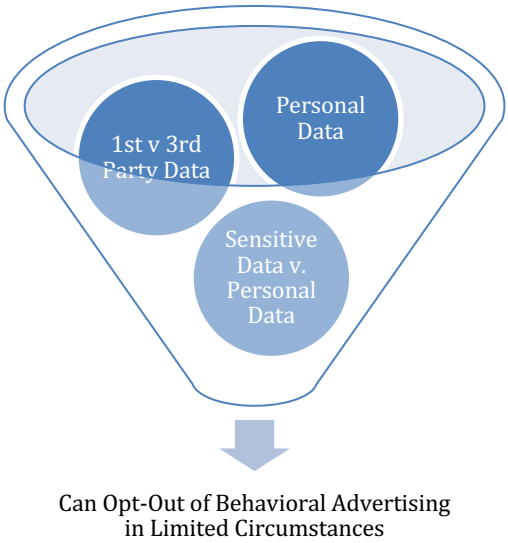
3. Other Gaps in Behavioral Advertising

As with the statutory right to opt out of profiling, we observe a similar funneling effect in how states address behavioral advertising, which limits the right's effectiveness and paradoxically increases the power of data-opolies.

decision made by the controller that results in the provision or denial by the controller of: (A) financial and lending services; (B) housing, insurance, or health care services; (C) education enrollment; (D) employment opportunities; (E) criminal justice; or (F) access to basic necessities, such as food and water"); *Virginia Consumer Data Protection Act*, Va. Code § 59.1-575 (defining term as "a decision made by the controller that results in the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water").

[278] *Colorado Privacy Act*, CO Revised Statutes § 6-1-1303(10) (defining term as "a decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services").

[279] STUCKE, BREAKING AWAY, *supra* note, at 108.



a. First-Party Versus Third-Party Personal Data

Residents in 20 states can opt out of targeted advertising. But 19 states define "targeted advertising" to exclude first-party personal data,[280] which is data the firm directly collects from individuals from its services and apps, such as the geolocation data Google collects when one uses Google Maps or Waze. Residents can only opt out of firm's use the third-party personal data, which refers to the information that firms collect when one visits other websites, apps, and sources, such as the data Google and Meta collect when one visits any of the 100,000 websites with their trackers.[281]

For example, the Iowa Consumer Data Protection Act defines targeted advertising as "displaying advertisements to a consumer where the advertisement is selected based on personal data obtained

[280] *Colorado Privacy Act*, CO Revised Statutes § 6-1-1303(25); Conn. Gen. Stat. Ann. § 42-515(28); *Delaware Personal Data Privacy Act*, Del. Code Ann. tit. 6, § 12D-102(33); *Kentucky Consumer Data Protection Act*, Ky. Rev. Stat. Ann. § 367.3611(30); Florida Digital Bill of Rights, Fla. Stat. Ann. § 501.702(33); *Iowa Consumer Data Protection Act*, Iowa Code Title XVI, Subtit. 1, Ch. 715D, § 715D.1(28); *Maryland Online Data Privacy Act*, Md. Code Ann., Com. Law § 14-4701(hh); *Minnesota Consumer Data Privacy Act*, Minn. Stat. Ann. § 325M.11(x); *Montana Consumer Data Privacy Act*, Mont. Code Ann. § 30-14-2802(25)(a); *Nebraska Data Privacy Act*, Neb. Rev. Stat. Ann. § 87-1102(32); *New Hampshire Expectation of Privacy*, N.H. Rev. Stat. Ann. § 507-H:1(XXIX); N.J. Stat. Ann. § 56:8-166.4; *Oregon Control and Processing of Consumer Personal Data Act*, Or. Rev. Stat. Ann. § 646A.570(19); *Rhode Island Data Transparency and Privacy Protection Act*, R.I. Gen. Laws Ann. § 6-48.1-2(27); *Tennessee Information Protection Act*, Tenn. Code Ann. § 47-18-3201(28); *Texas Consumer Data Protection*, Tex. Bus. & Com. Code Ann. § 541.001(31); *Utah Consumer Privacy Act*, Utah Code § 13-61-101(35)(a); *Virginia Consumer Data Protection Act*, Va. Code § 59.1-575.

[281] *See, e.g.*, In re BPS Direct, LLC, 705 F. Supp. 3d 333, 344 (E.D. Pa. 2023) (distinguishing first-party cookies "created by the website the user is visiting" and third-party cookies "created by a different website than the one the user is visiting").

from that consumer's activities over time and across *nonaffiliated* websites or online applications to predict such consumer's preferences or interests."[282] To avoid any ambiguities, the Act excludes from "targeted advertising" the following:

> a. *Advertisements based on activities within a controller's own or affiliated websites or online applications.*
>
> *b. Advertisements based on the context of a consumer's current search query, visit to a website, or online application.*
>
> *c. Advertisements directed to a consumer in response to the consumer's request for information or feedback.*
>
> *d. Processing personal data solely for measuring or reporting advertising performance, reach, or frequency.*[283]

So, residents in these 19 states cannot opt out of behavioral advertising generally. Instead, residents can prevent firms from using one category of personal data for these ads. In California, residents can opt out of having their sensitive personal information (regardless of whether it is first- or third-party data) being used for behavioral advertising.[284] Otherwise, Californians cannot opt out of targeted advertising using any first-party data that is not considered "sensitive."[285]

Although the opt-out right has some benefits,[286] one significant downside is the statutory

---

[282] Iowa Code Title XVI, Subtit. 1, Ch. 715D, § 715D.1(28) (emphasis added). The Act defines "affiliate" as "a legal entity that controls, is controlled by, or is under common control with another legal entity or shares common branding with another legal entity. For the purposes of this definition, 'control' or 'controlled' means: a. Ownership of, or the power to vote, more than fifty percent of the outstanding shares of any class of voting security of a company; b. Control in any manner over the election of a majority of the directors or of individuals exercising similar functions. c. The power to exercise controlling influence over the management of a company."

[283] *Id*. The other state privacy laws generally track that language, except Florida's Digital Bill of Rights, Fla. Stat. Ann. § 501.702(33) (excluding advertisements that are (a) "Based on the context of a consumer's current search query on the controller's own website or online application; or (b) Directed to a consumer search query on the controller's own website or online application in response to the consumer's request for information or feedback").

[284] Cal. Civ. Code § 1798.121.

[285] *Id*. § 1798.140(k) (excluding first-party data from its definition of "cross-context behavioral advertising," which means "the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts").

[286] The opt-out right reduces the incentive for cross-platform tracking and will require firms to better account for the data they collect. For example, the FTC found in its investigation of social media sites that none provided a comprehensive list of all third-party entities with whom they shared personal data. FTC 2024 Report, *supra* note, at 25. "Some Companies provided illustrative examples, whereas others claimed that this request was impossible." *Id*. When residents opt out of sharing their data with third parties and cross-platform tracking for behavioral advertising, firms must account with whom they shared personal data and for what purpose.

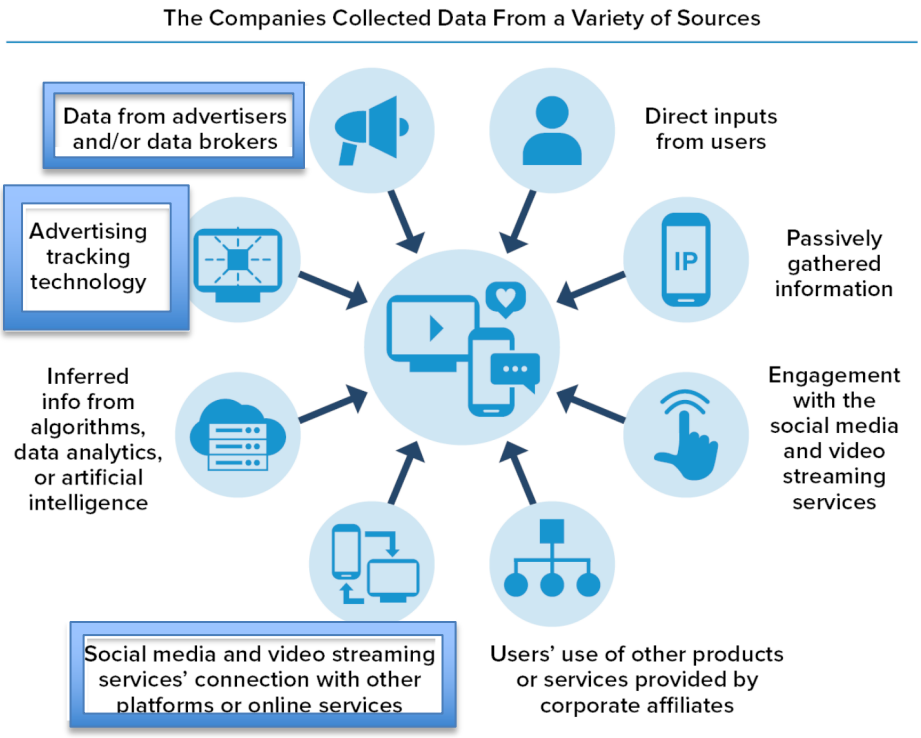
distinction between first- and third-party data, which paradoxically will hinder smaller firms and benefit those data-opolies that already yield supra-competitive profits from behavioral advertising.

The "walled gardens," as we saw in Part I.C., compete against millions of websites and apps for behavioral advertising revenues. The aim of behavioral advertising is to target individuals with the right ad at the right time, thereby inducing them to undertake the desired action. Such targeting depends on continually predicting behavior and learning from the predictions. For example, did the person, when targeted with a personalized ad for Twinkies, stop at the nearby convenience store? Predicting through trial and error requires updating the AI model with personal data. The flywheel effects already benefit the data-opolies, as they collect more first-party data to profile users and sustain their attention while manipulating and monetizing their behavior.

For many apps and websites outside the walled gardens, this involves monitoring what individuals do after leaving their website and app. To effectively monitor, the open web relies more heavily on third-party data obtained from tracking software, such as pixels[287] and cookies, about the person's activities on other websites. By allowing individuals to opt out of targeted advertising based on third-party data, the states are effectively hindering the efforts of millions of publishers and apps.

To see why, consider the FTC's chart of the eight different categories of data that social media firms collect:

[287] FTC Office of Technology, Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking (March 16, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking.



Source: FTC Staff Report, A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services, at 21(Sept. 2024)

Of the eight categories, three (which are bracketed) involve third-party data, while the remaining five categories involve first-party data, which can still be used for behavioral advertising. The leading walled gardens, Google, Meta, and Amazon, collect relatively more first-party data than what each independent app and website collects. For example, Google harvests personal data from --

- Its seven products, which by 2024 had over 2 billion users each: (i) Android, the world's most popular operating system, with over 3 billion active devices worldwide,[288] (ii) Google Maps, (iii) Chrome, (iii) Gmail, (iv) Maps, (v) Play Store, (vi) Search, and (vii) YouTube, the most-watched streaming service in the US;[289]
- Its 40+ other services for users, including Google Drive and Google Photos;[290]
- Its Pixel devices, including phones, buds, tablets, and watches;
- Its home and smart appliances (through its digital assistant Google Home and

[288] Letter to Shareholders, Alphabet 2024 10-K at 2

[289] *Id.*; Alphabet 2024 10-K at 1.

[290] https://about.google/products/

Google Nest security cameras, doorbells, and smart thermostats)[291];

- Cloud computing service Google Cloud;
- Verily ("an Alphabet data platform and technology company purpose-built to power AI for precision health" by offering "AI-enabled solutions that transform disparate health data into insights and actions that accelerate research and improve care for individuals and communities");[292] and
- Third parties (including the analytical technology Google places on millions of third-party websites and apps).

So, if a resident in these 19 states opts out of targeted advertising, Google could still use all the above categories of personal data for behavioral advertising except the last category. Granted, Google and Meta will have less personal data as a result (as they can no longer use the data flowing from the 100,000+ third-party websites on which they have trackers for residents who opted out of behavioral advertising). But these walled gardens will collect far more current first-party data than the atomistic websites and apps, thereby widening their already significant competitive advantage for behavioral advertising revenue.

AI will widen that competitive gap even further. Developers of generative AI models, the OECD noted, "are increasingly facing data scarcity, despite extensive and increasingly controversial web scraping practices to obtain data."[293] Key here is AI powered by first-party data.[294] The AI model "synthesizes trillions of behavioral signals into intent-based scores tied to a unique individual."[295] For the leading social media firms, one important source of data, as the FTC found, is information inferred by AI. Smaller firms can rely on platforms like Zeta, Outbrain, and Taboola for inferred data. But the first-party data from each firm, while voluminous, will likely pale against the volume and variety of first-party data that the walled gardens collect and the velocity in which the walled gardens' AI models can be trained, fine-tuned, and updated with this first-party data.

For example, by 2024, Google had incorporated its foundation model, Gemini, into 15 Google products, serving half a billion users.[296] Moreover, Google is integrating its foundation model into

---

[291] https://store.google.com/us/category/connected_home?hl=en-US

[292] https://verily.com/perspectives/verily-welcomes-new-workbench-organizations-to-manage-biomedical-datasets-and-accelerate-research.

[293] OECD, Policy Brief: Enhancing Access to and Sharing of Data in the Age of Artificial Intelligence (Feb. 6, 2025).

[294] Zeta 2024 10-K, *supra* note; July 24, 2024 Interpublic Group of Companies, Inc. conference call to discuss its second-quarter and first-half 2024 results (CEO stating: "In a world in which data-driven audience insights are key to delivering performance for our clients, and one in which Al will play an increasingly important role, access to high-quality, proprietary data at scale will be essential to success.").

[295] Zeta 2024 10-K, *supra* note, at 3.

[296] Letter to Shareholders, Alphabet 2024 10-K, *supra* note, at 1.

its other popular products, such as its search engine, which performs approximately 16.4 billion searches every day (which translates to 189,815 searches per second).[297] Thus, Google's AI will likely be trained by the first-party data of over 2 billion users worldwide.[298] By 2024, over 1.5 billion people used Google's AI Overviews each month, its AI complement to its search engine results.[299] And the search queries on AI Overview differ from its search engine, as the AI Mode search queries "are twice as long as traditional Search queries."[300]

So, as Google integrates its AI into more products, more people will interact with its foundation model, which provides even more opportunities for the foundation model to gather even more first-party data to profile individuals, target them with behavioral ads, and manipulate their behavior, such as which YouTube videos will likely sustain that individual's attention. In contrast, independent websites and apps will unlikely have their own AI foundation models. Even if they did, their models would have far less first-party data on which to train. Nor can the websites and apps use third-party personal data to train their foundation model for behavioral advertising purposes for residents who opted out.

Thus, state laws paradoxically reward those dominant ecosystems that already leverage their first-party data advantage, which they collect across their interconnected platforms, products, and services to target users with behavioral ads.[301] Indeed, the laws increase these data-opolies' incentives to expand their ecosystems, to capture even more first-party data to train their AI to find more ways to capture even more of our attention and behavioral advertising revenues. The longer we stay in their ecosystems, the more first-party data they collect, the more opportunities to predict and manipulate our behavior, and the more money they make.

b. Sensitive Data versus Personal Data

As the FTC found, targeted advertising based on sensitive categories of personal data "can be extremely harmful to consumers and cause a wide range of injuries to users," including "unlawful

---

[297] https://explodingtopics.com/blog/google-searches-per-day. *Google*, 747 F. Supp. 3d at 49–50, 51 (noting that Google's greater query volume means more user data; as the most widely used general search engine in the US, "Google receives nine times more queries each day than all of its rivals combined across all devices," that the disparity was even more pronounced on mobile, where Google receives "nineteen times more queries than all of its other rivals put together," and the thirteen months of user data acquired by Google was equivalent to over 17 years of data on Microsoft's search engine Bing).

[298] Letter to Shareholders, Alphabet 2024 10-K at 2; Alphabet 2024 10-K, *supra* note, at 1.

[299] https://abc.xyz/2025-q1-earnings-call/

[300] *Id*.

[301] Kak & West Statement, *supra* note (noting that "unlike other actors that must largely rely on third-party intermediaries to access data, large firms are exploiting the fact that they directly control the vast majority of the environment in which data is collected; they are able to take advantage of the network effects associated with the scale at which they operate by collecting, analyzing, and using data within platforms they wholly own and control," and how this "is a product of a self-reinforcing feedback loop, which over time has led to these firms being so dominant and pervasive that it is virtually impossible not to use their systems").

discrimination, emotional distress, stigma, reputational harm, embarrassment, and invasion of privacy."[302] As a result, like the GDPR, the twenty states with privacy laws impose greater responsibilities and restrictions on categories of personal data that are deemed sensitive. Firms cannot process their residents' sensitive data without first obtaining the resident's consent[303] or (in a few states) allowing the resident to opt out.[304]

However, even this right, coupled with the other opt-out rights, will not prevent the harms of AI profiling and behavioral advertising for several reasons.

First, the laws do not allow residents to opt out of profiling or behavioral advertising generally. Residents must simply give their consent if their sensitive data is being processed for, among other things, profiling them and behavioral ads. Therefore, one may encounter the same criticisms of privacy's notice and consent regime, where residents do not read the lengthy, opaque privacy notices and simply consent.[305]

Second, the notice and consent regime is ineffective when consumers lack viable alternatives. This is likely when firms have significant market power or when incentives are misaligned. Under either scenario, residents cannot exercise sufficient control to delineate towards which use their sensitive personal data may be put and not put. For example, to use Google Maps, one might have

---

[302] FTC 2024 Report, *supra* note, at 44.

[303] *Colorado Privacy Act*, CO Revised Statutes § 6-1-1308(7); *Connecticut Consumer Data Privacy and Online Monitoring Act,* Conn. Gen. Stat. Ann. § 42-520(a); *Delaware Personal Data Privacy Act*, Del. Code Ann. tit. 6, § 12D-106(a)(4); *Florida Digital Bill of Rights*, Fla. Stat. Ann. § 501.71(2)(d); *Indiana Consumer Data Protection Act*, Ind. Code Ann. § 24-15-4-1; *Kentucky Consumer Data Protection Act*, Ky. Rev. Stat. Ann. § 367.3617(1)(e); *Minnesota Consumer Data Privacy Act*, Minn. Stat. Ann. § 325O.07; *Montana Consumer Data Privacy Act*, Mont. Code Ann. § 30-14-2812(2)(b); *Nebraska Data Privacy Act*, Neb. Rev. Stat. Ann. § 87-1112(2)(d); *New Hampshire Expectation of Privacy*, N.H. Rev. Stat. Ann. § 507-H:6(I)(d); N.J. Stat. Ann. § 56:8-166.12; *Oregon Control and Processing of Consumer Personal Data Act*, Or. Rev. Stat. Ann. § 646A.578(2)(b); *Rhode Island Data Transparency and Privacy Protection Act*, R.I. Gen. Laws Ann. § 6-48.1-4(c); *Tennessee Information Protection Act*, Tenn. Code Ann. § 47-18-3204(a)(6); *Texas Consumer Data Protection*, Tex. Bus. & Com. Code Ann. § 541.101(b)(4); *Virginia Consumer Data Protection Act*, Va. Code § 59.1-578(A)(5).

[304] *California Consumer Privacy Act*, Cal. Civ. Code § 1798.121; *Iowa Consumer Data Protection Act*, Iowa Code Title XVI, Subtit. 1, Ch. 715D, § 715D.4(2); *Utah Consumer Privacy Act*, Utah Code §§ 13-61-302(3). Maryland's Online Data Privacy Act takes a different approach to sensitive data, where a controller can collect or process sensitive data only when "strictly necessary to provide or maintain a specific product or service requested by the consumer." The controller may process personal data for other purposes if it obtains the consumer's consent. Md. Code Ann., Com. Law §§ 14-4707(a)(1) & (8).

[305] *See, e.g.*, FTC 2024 Report, *supra* note, at 38 (noting how social media companies' "privacy notices can frequently be lengthy, vague, and generally unhelpful;" how FTC attorneys and technologists with privacy expertise were "often unable to decipher such policies and notices and clearly ascertain the Companies' actual practices," and given that, how the privacy notice provided to consumers was "illusory, and consumers cannot truly make a choice"); Solove, *supra* note, at 19-20 (noting how countless privacy experts have attacked the notice-and-choice approach for being ineffective, and for some, downright farcical); Caitlin Chin, *Current U.S. Privacy Laws Fail to Check U.S. Data Broker Partnerships with Government Agencies*, *in* SURVEILLANCE FOR SALE: THE UNDERREGULATED RELATIONSHIP BETWEEN U.S. DATA BROKERS AND DOMESTIC AND FOREIGN GOVERNMENT AGENCIES at 14 (Center for Strategic and International Studies 2023), https://www.jstor.org/stable/resrep51658.7.

to consent to Google's use of one's geolocation data (which many states deem sensitive) for both functionality (e.g., assess traffic patterns) and behavioral advertising purposes. Google may not offer residents the opportunity to specify which uses of their geo-location data that Google can or cannot use.

Third, the states define sensitive data differently. Many states define "sensitive data" as a category of personal information that includes

- Personal information revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis [some states add the qualifier *made by a health care provider*[306]], sexual orientation [and, in some states, *sex life*[307]], or citizenship or immigration status [with the caveat in some states *except to the extent such data is used in order to avoid discrimination on the basis of a protected class that would violate a federal or state anti-discrimination law*[308]];
- The processing of genetic or biometric data for the purpose of uniquely identifying a natural person;
- The personal information collected from a known child;[309] or
- Precise geolocation data.[310]

Colorado's definition of sensitive data includes biological data[311] and neural data.[312] Oregon's definition includes personal data that reveals a consumer's "status as transgender or nonbinary" and "status as a victim of crime."[313] Connecticut's definition includes data revealing "mental or

---

[306] Indiana IC 24-15 § 28.

[307] *Montana Consumer Data Privacy Act*, Mont. Code Ann. § 30-14-2802(24); *New Hampshire Expectation of Privacy*, N.H. Rev. Stat. Ann. § 507-H:1(XXVIII); *Rhode Island Data Transparency and Privacy Protection Act*, R.I. Gen. Laws Ann. § 6-48.1-2(26).

[308] *Iowa Consumer Data Protection Act*, Iowa Code Title XVI, Subtit. 1, Ch. 715D, § 715D.1(26); *Utah Consumer Privacy Act*, Utah Code §§ 13-61-101(32)(a)

[309] Excluded from the definition in Utah Code § 13-61-101(32)(a) but recaptured in § 13-61-302(3)(b).

[310] *Florida Digital Bill of Rights*, Fla. Stat. Ann. § 501.702(31); *Kentucky Consumer Data Protection Act*, Ky. Rev. Stat. Ann. § 367.3611(28); *Minnesota Consumer Data Privacy Act*, Minn. Stat. Ann. § 325M.11(v); *Nebraska Data Privacy Act*, Neb. Rev. Stat. Ann. § 87-1102(30); *Tennessee Information Protection Act*, Tenn. Code Ann. § 47-18-3201(26); *Texas Consumer Data Protection*, Tex. Bus. & Com. Code Ann. § 541.001(29); *Virginia Consumer Data Protection Act*, Va. Code § 59.1-575.

[311] CO ST §§ 6-1-1303(24) & (2.2) (defining biological data as "data generated by the technological processing, measurement, or analysis of an individual's biological, genetic, biochemical, physiological, or neural properties, compositions, or activities or of an individual's body or bodily functions, which data is used or intended to be used, singly or in combination with other personal data, for identification purposes").

[312] *Id*. §§ 6-1-1303(2.2) & (16.7) (defining "neural data" as information that is "generated by the measurement of the activity of an individual's central or peripheral nervous systems and that can be processed by or with the assistance of a device").

[313] Or. Rev. Stat. Ann. § 646A.570(18)(a).

physical health condition," sex life, consumer health data,[314] and data concerning an individual's status as a victim of crime.[315] Finally, California defines "sensitive personal information" more broadly to include personal information that reveals:

- A consumer's social security, driver's license, state identification card, or passport number;
- A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;
- a consumer's religious or philosophical beliefs, or union membership;
- the contents of a consumer's mail, email and text messages, unless the business is the intended recipient of the communication;
- personal information collected and analyzed concerning a consumer's health; or
- personal information collected and analyzed concerning a consumer's sex life or sexual orientation.[316]

This disparity over what constitutes sensitive personal information extends beyond the twenty states. The leading social media firms, for example, claim in their privacy policies "to prohibit targeting based on sensitive categories, such as race, religion, sexual orientation, and political affiliation."[317] But the FTC found "an overall lack of consistency about which categories were considered sensitive and how the Companies described these prohibited forms of targeting in their policies."[318]

This divergence over what constitutes sensitive personal information can pose challenges for firms seeking to comply with these laws. Suppose Meta's AI can infer whether someone belongs to a union. Before processing that information, must Meta get the individual's consent? That depends in part on the person's legal residence. Thus, the disparity over what is and is not "sensitive" can cause confusion among individuals and firms regarding what is and is not subject to greater restrictions; it can also lead to uneven enforcement of individuals' rights.

Fourth, as we have seen with public and non-public data, AI can blur the line between sensitive personal data and other types of data. As Part I discusses, AI can infer from non-sensitive data information that is deemed sensitive under state law.[319] Individuals may incorrectly assume that

---

[314] Conn. Gen. Stat. Ann. § 42-515(9) (defining "consumer health data" as any personal data that a controller uses to identify a consumer's physical or mental health condition or diagnosis, and includes, but is not limited to, gender-affirming health data and reproductive or sexual health data").

[315] *Id*. § 42-515(38).

[316] Cal. Civ. Code § 1798.140(ae).

[317] FTC 2024 Report, *supra* note, at 44.

[318] *Id*.

[319] Kosinski et al., *supra* note.

by withholding their consent, they can protect their sensitive information. But their consent may not be needed when a firm's AI infers this sensitive information from the non-sensitive information it ingests. Here again, the data-opolies will likely benefit: they have a greater volume and variety of non-sensitive first-party personal data to train and fine-tune their AI models, which can then infer more sensitive information about individuals from this first-party data.[320] This renders the limited opt-in right meaningless when the powerful wall gardens can use these inferences for profiling and behavioral advertising.[321]

Finally, with AI tapping into emotional advertising, the delineation between sensitive and non-sensitive data may be even less meaningful. For example, California defines biometric data, which includes facial expressions, as sensitive if processed "for the purpose of uniquely identifying a consumer."[322] However, under California law, companies can use customers' facial expressions to assess their emotions and adjust advertising in real time to manipulate their behavior.

* * *

Consequently, the states have not imposed adequate guardrails to curb profiling and behavioral advertising and the misaligned incentives they create. As of mid-2025, residents cannot opt out of AI profiling or behavioral advertising generally. They can only limit the use of some categories of data for behavioral advertising, and only some types of profiling. In California, residents can opt out of behavioral advertising for some first-party data that is sensitive under that law. Otherwise, individuals cannot effectively opt out of the collection and use of publicly available or first-party personal data to profile them, target them with behavioral ads, and manipulate their behavior.

C. Right to Delete One's Data

An alternative, albeit not ideal, is for residents to delete their data under the state's privacy law or the company's privacy policy.[323] But four issues remain.

---

[320] FTC 2024 Report, *supra* note, at 62.

[321] Some states might be the exception. California's privacy law defines sensitive information "as personal information that reveals" the various categories mentioned earlier. Cal. Civ. Code § 1798.140(ae). Its definition of personal information includes "[i]nferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes." *Id*. § 1798.140(v)(1)(K). Thus, inferences from non-sensitive personal data that reveal sensitive categories of information could be "sensitive information" if used in a profile. But the law specifically excludes "publicly available" data from its definition of sensitive data, so even in California, AI can infer sensitive information from "publicly available" data. In Colorado, controllers generally must obtain consent to process Sensitive Data, including Sensitive Data Inferences, with some exceptions. Colorado Privacy Act Rule 6.10, 4 CCR 904-3, https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf.

[322] Cal. Civ. Code § 1798.140(ae).

[323] Glenn A. Brown, Consumers' "Right to Delete" under US State Privacy Laws, Squire Patton Boggs, March 3,

First, what data can be deleted? In California, for example, residents can only delete the personal data that they provided to the controller.[324] A resident cannot delete publicly available data, data that the controller has collected from third parties, or data inferred about the individual.

Second, what does it mean to delete? Upon request, presumably, the company would permanently erase one's personal data. However, as the FTC found in its investigation of the leading social media companies, "this understanding is not in line with several Companies' reported practices."[325] For example, some companies claimed to de-identify the data rather than delete it.[326] Even those companies "that reported permanently erasing user data nevertheless conceded that they did not delete all data submitted by a user, such as user-generated content that is public."[327] As we saw, state privacy laws do not protect de-identified and publicly available data.

Third, with AI, one must ask exactly what exactly is being deleted. The AI foundation models may not store the data on which they are trained, and few, if any, employees may know on what specific data the model was trained or fine-tuned. As OpenAI noted, "Much like a person who has read a book and sets it down, our models do not have access to training information after they have learned from it."[328]

California amended in 2024 its privacy law "to underscore that personal information . . . can exist in various formats, including but not limited to . . . [a]bstract digital formats, including compressed or encrypted files, metadata, information."[329] California's amendment "seeks to underscore that personal information that exists in AI systems is still personal information, and therefore subject to existing CCPA obligations on businesses, such as data minimization, and the requirement to respond to consumer requests to access, delete, correct, and stop the sale/sharing of their personal information."[330]

But left unanswered is whether the personal information exists in ChatGPT, given that the foundation model no longer has access to this source data. Returning to our example, the *Wall Street Journal* article used to train the AI model may or may not "exist" in the foundation model,

---

2021, https://www.privacyworld.blog/2021/03/consumers-right-to-delete-under-us-state-privacy-laws/; Google Privacy & Terms, https://policies.google.com/technologies/retention?hl=en-US.

[324] Cal. Civ. Code § 1798.105(a) (limiting consumers' right to request a business to delete any personal information about them to information "collected from the consumer").

[325] FTC 2024 Report, *supra* note, at 33.

[326] *Id*.

[327] *Id*.

[328] White, *supra* note.

[329] Memorandum dated July 11, 2024 to the California Privacy Protection Agency Board (Meeting of July 16, 2024) from Maureen Mahoney, Deputy Director of Policy & Legislation, California Privacy Protection Agency re: Agenda Item 7— Legislative Update and Possible Authorization for CPPA's Positions on Pending Legislation. AB 1008 (Bauer-Kahan), California Consumer Privacy Act of 2018: personal information, as amended June 24, 2024).

[330] *Id*.

just as fragments of news articles that one read years ago may "exist" in one's thoughts, even though one cannot retrieve the article. Thus, even if the incriminating *Journal* article were considered personal data under the state statute, it is questionable how a resident can request that OpenAI access or delete that personal information (without deleting the entire ChatGPT model). Consequently, even if the company deletes the personal data on which the foundation model was trained, the AI model can continue to draw inferences about the individual. As the OECD noted,

> *A question that arises then is whether the privacy rights of individuals are adequately tailored to address these concerns ex post. For instance, if a "hallucination" includes inaccurate information including personal data generated by AI, do individuals have a right to have their data corrected and/or deleted? And if the identification and deletion of specific data sets from an AI model is extremely complex, both technically and logistically, to the point of rendering the right of rectification not possible in practice, should then the entire AI model, including the personal data in question, be deleted? As this example shows, it is still difficult to fully appreciate both the privacy risks and the consequences of the application of privacy laws to AI models in the current state of the art.*[331]

Finally, the right to delete does not stop profiling and behavioral advertising; instead, exercising this right becomes for residents a "Sisyphean task." Sisyphus, according to Greek legend, was condemned to the endless task of rolling an immense boulder up a steep hill, only for the boulder to roll back down. Suppose individuals delete their personal data. The company can continue profiling and immediately create a new one (if the privacy law even allows individuals to delete their profiles). AI can expedite this function, as the individual can quickly be placed in a look-alike audience (of all the residents who have not deleted their profiles). Like Sisyphus, the individual must repeat the task to minimize (but not prevent) profiling and behavioral advertising. Unlike Sisyphus, who had only one boulder with which to contend, individuals would have to continually delete their data from thousands of websites and apps without coming to any privacy resolution.

* * *

The good news is that twenty states across the political divide have been more adept than Congress in providing their residents with greater control over their data. However, these laws, while well-intentioned, will not significantly curb this toxic competition. Instead, the laws may have the unintended consequence of benefitting data-opolies.

---

[331] OECD AI Report, *supra* note, at 21.

Nor has Europe curtailed the harms of profiling and behavioral advertising. In 2016, the European Union adopted the General Data Protection Regulation (GDPR), which it promoted as "one of its greatest achievements in recent years."[332] Two years later, its member states fully implemented the privacy law. What impact, if any, did the GDPR have on behavioral advertising? It is hard to see any effect. Meta, as we saw, relies on behavioral advertising for nearly all its revenues. In its first quarter of 2018, Meta generated $11.795 billion in behavioral advertising worldwide, with $2.992 billion coming from EU users and $5.559 billion from users in the US and Canada.[333] Fast forward to the first quarter of 2025: Meta's advertising revenues more than doubled from users in Europe (218% to $9.527 billion), as well as users in the US and Canada (228% to $18.259 billion) and users worldwide (251% to $41.392 billion).[334] After the GDPR, Google remained in the lead with its trackers found on 81% of the EU websites, followed by Meta (with trackers on 44% of the EU websites).[335] So why didn't the GDPR curb behavioral advertising? One reason was shortcomings in the GDPR itself.[336] Another factor was the ineffective enforcement of the Irish Data Protection Commission, which has jurisdiction over Google and Meta.[337] But that may be changing in the EU.[338] However, as the next Part addresses, the states need not replicate the

---

[332] European Data Protection Supervisor, The History of the General Data Protection Regulation, https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

[333] Facebook Q1 2018 Results, https://s21.q4cdn.com/399680738/files/doc_financials/2018/Q1/Q1-2018-Earnings-Presentation-(1).pdf

[334] Comparing "Advertising Revenue by User Geography in Millions" https://s21.q4cdn.com/399680738/files/doc_financials/2025/q1/Earnings-Presentation-Q1-2025-FINAL.pdf

[335] STUCKE, BREAKING AWAY, *supra* note, at 100.

[336] For some of the GDPR's historical shortcomings in curbing behavioral advertising, see id. at 101, 136-47; see also OECD Note from Italy, *supra* note, at 3 (noting practical challenges of adhering to GDPR principles, like data minimization, purpose limitation, and storage limitation "in the context of massive data collection by digital firms," where often "the purposes for data processing are broadly defined, complicating compliance efforts").

[337] STUCKE, BREAKING AWAY, *supra* note, at 143; WYNN-WILLIAMS, *supra* note, at 175-76 (discussing Facebook's friendly relationship with Ireland's prime minister who asked Meta to build up the credibility of the nation's privacy agency as a pit bull, when in fact it was more of a lapdog).

[338] In 2023 and 2024, the European Court of Justice curtailed Meta's ability to indefinitely collect data on and off its platforms for behavioral advertising, finding that "such processing is particularly extensive since it relates to potentially unlimited data and has a significant impact on the user, a large part – if not almost all – of whose online activities are monitored by Meta Platforms Ireland, which may give rise to the feeling that his or her private life is being continuously monitored." Schrems v. Meta, case number C-446/21, 4 October 2024, quoting judgment of 4 July 2023, Meta Platforms and Others (General terms of use of a social network), C-252/21, EU:C:2023:537, paragraph 118). Moreover, Article 5 of the EU's Digital Markets Act enables Europeans to manage better their personal data controlled by dominant firms (deemed gatekeepers under the Act). The gatekeeper, absent the user's consent, cannot: (a) "process, for the purpose of providing online advertising services, personal data of end users using services of third parties that make use of core platform services of the gatekeeper; (b) combine personal data from the relevant core platform service with personal data from any further core platform services or from any other services provided by the gatekeeper or with personal data from third-party services; (c) cross-use personal data from the relevant core platform service in other services provided separately by the gatekeeper, including other core platform services, and vice versa; and (d) sign in end users to other services of the gatekeeper in order to combine personal data." Meta's core platform services (Facebook, Instagram, WhatsApp, Messenger, and Meta Ads) have been designated gatekeepers.

GDPR. Instead, they can make a few revisions to their existing statutes to better protect their residents from harmful profiling and behavioral advertising.

III. WHAT SHOULD BE DONE?

Federal legislation should provide minimum privacy safeguards for every citizen.[339] But some Republican Congressmen in 2025 were more intent on stopping the states from enforcing any law regulating AI models for at least a decade,[340] than in protecting residents from AI-profiling and behavioral advertising. Congress, as composed in mid-2025, seems incapable of providing intelligible privacy safeguards. Therefore, this Article turns to the 20 states that can amend their existing privacy laws (and the remaining states that still have not passed comprehensive privacy laws) to provide the needed guardrails to realign incentives and encourage more firms to compete on privacy.

As a senior FTC official observed in 2024, "to fix the system, fix the incentives."[341] The FTC's findings of the social media companies "should not be viewed in isolation," he noted, as "[t]hey stem from a business model that varies little across these nine firms – harvesting data for targeted advertising, algorithm design, and sales to third parties. With few meaningful guardrails, companies are incentivized to develop ever-more invasive methods of collection."[342] He is not alone. Others, including the ICN Privacy/Competition Report, have highlighted the race to the bottom resulting from these misaligned incentives.[343] To realign incentives, states should close

---

https://digital-markets-act.ec.europa.eu/gatekeepers_en As a result, Instagram and Facebook users in Europe can manage their accounts so that Meta no longer uses their information across accounts. https://about.fb.com/news/2024/01/offering-people-more-choice-on-how-they-can-use-our-services-in-the-eu/. German users also received this right because of the Bundeskartellamt's successful prosecution of Meta under its competition laws. For a case summary, see STUCKE, BREAKING AWAY, *supra* note, at 139-42.

[339] Even a federal remedy will have issues, such as whether individuals with a private cause of action would likely have standing under Article III of the Constitution, under the Supreme Court's convoluted standard for intangible privacy harms. *See, e.g.*, Thornley v. Clearview AI, Inc., 984 F.3d 1241, 1250 (7th Cir. 2021) (Hamilton, J., concurring) (noting lack of clarity from courts' opinions on whether plaintiffs have standing for intangible privacy harms, which stems from the Supreme Court's Delphic instruction that standing requires ''concrete'' injury but that ''intangible injuries can nevertheless be concrete,'' and confessing that he has "not yet been able to extract from these different lines of cases a consistently predictable rule or standard").

[340] Matt Stoller, *Will Congress Legalize Mark Zuckerberg As Your Therapist?*, BIG, May 14, 2025, https://www.thebignewsletter.com/p/will-congress-legalize-mark-zuckerberg?emci=07f3f0f6-c047-f011-8f7c-6045bdfe8e9c&emdi=84146c29-c747-f011-8f7c-6045bdfe8e9c&ceid=15514063

[341] Preface by Samuel Levine, Director, Bureau of Consumer Protection, FTC, to FTC Staff Report, *supra* note.

[342] *Id*.

[343] *See, e.g.*, OECD Note from Italy, *supra* note, at 7 (noting that instead "of fostering environments that protect individual privacy, firms often engage in a competitive race to extract and use personal data, exploiting consumers to maximize profits"); U.S. Senator Maria Cantwell, Opening Statement, Senate Committee on Commerce, Science, and Transportation, Hearing: The Need to Protect Americans' Privacy and the AI Accelerant (July 11, 2024) (incentives create "race to the bottom where the most privacy protective companies are at a competitive disadvantage"); Tiwari

several loopholes in their privacy laws regarding behavioral advertising and profiling.

A. Require Opt-in of All Behavioral Advertising

First, regarding behavioral advertising, the states should eliminate the distinctions among first-party personal data, third-party personal data, and publicly available data. Targeted advertising should be defined more broadly as displaying advertisements to a consumer where the advertisement is selected based on personal data, including publicly available data obtained or inferred from that consumer's activities over time and across websites or online applications, to predict the consumer's preferences or interests.[344] To avoid any ambiguities, "targeted advertising" should include ads based on (i) activities within a controller's own or affiliated websites or online applications, and (ii) processing personal data solely for measuring or reporting advertising performance, reach, or frequency. The laws could, as they do currently, exclude as "targeted advertising" (a) contextual advertisements based on the context of a consumer's current search query, or visit of that website or online application and (b) advertisements directed to consumers in response to their request for information or feedback.

The next issue is whether residents should have to opt out of behavioral advertising rather than opting in. Under an opt-in regime, the default is no surveillance and profiling for behavioral advertising. Elsewhere, I have argued for banning behavioral advertising (or at a minimum making it opt-in),[345] which is consistent with the survey data.[346] This protects residents from data brokers who collect their data without their knowledge.

Indeed, some states are enacting and amending their privacy laws to protect teenagers and minors by requiring them (or for those under 13 their guardians) to opt into behavioral advertising. Take, for example, Connecticut. Originally its privacy law required businesses to obtain consent from

---

Statement, *supra* note (testifying that "a comprehensive privacy legislation is foundational to any sound AI framework" and that "[w]ithout such legislation, we risk a 'race to the bottom' where companies compete by exploiting personal data rather than safeguarding it"); Open Markets Institute & Center for Journalism and Liberty, Submission to the Office of Science and Technology Policy's Request for Information on the Development of an Artificial Intelligence (AI) Action Plan (March 15, 2025); Kak & West Statement, *supra* note (noting that "tech firms already have strong incentives for irresponsible and invasive data collection, fueled primarily by a business model that relies on personalized behavioral targeting of consumers with advertising" and warning that "AI boom exacerbates this, fueling a race to the bottom").

[344] *See, e.g.*, Thomas Ploug, *People Should Have a Right Not to be Subjected to AI Profiling Based on Publicly Available Data: A Reply to Holm*, 36 PHILOSOPHY & TECHNOLOGY 49 (2023), https://doi.org/10.1007/s13347-023-00652-5 (arguing that "AI profiling based on publicly available data is exceptional, it could be considered an independent category of data use in a meta consent model, and thus, a category of data for which a particular kind of consent request should be made").

[345] STUCKE, BREAKING AWAY, *supra* note, at 209-11.

[346] See *supra* note **.

consumers who were 13 to 15 years old before sending them targeted ads.[347] But it did not protect 16- to 17-year-olds. In amending its law, the legislators noted the decline in well-being among minors:

> *Researchers have found the wellbeing of America's youth in an alarming state. According to a 2024 report by the CDC, 53% of high school girls in 2023 reported feeling "persistently sad or hopeless" over the previous year, up from 36% in 2011. Meanwhile, 27 percent of high school girls seriously considered attempting suicide in 2021, up from 19% in 2011.*
>
> *Social media use by teens took off in that time frame, in a trend that began before the COVID-19 pandemic. Studies suggest there is a strong negative correlation between mental health and social media use.*
>
> *As youth mental health metrics have declined, tech companies have employed the personal data of minors to target them with advertisements, to lure them into scrolling longer, or encourage them to continue watching videos.*
>
> *From 2019 to 2021, youth increased their screen time 17%, which encompassed an average of 5 hours and 33 minutes daily for those 8 to 12 years old, and 8 hours and 39 minutes for those 13 to 18 years old.* [348]

In 2024, Connecticut enacted a new law, modeled in part on the UK's Age-Appropriate Design Code, which requires websites that offer online service to minors to use reasonable care to avoid a "heightened risk" of harm to young people.[349] The 2024 law bans targeted advertisements and the sale of data generated by users under the age of 18 without opt-in consent.[350] The new law also prohibits "features designed to significantly increase a minor's use of the online service, i.e., endless scrolling habits, prohibit collection of geo-location data without opt-in consent, and ban unsolicited direct messaging from an adult to an unknown minor."[351]

Likewise, the FTC amended in 2025 its rules under the Children's Online Privacy Protection Act of 1998 to prevent firms from indefinitely retaining children's personal data and require separate opt in consent for targeted advertising to children under the age of 13.[352]

---

[347] C.G.S.A. § 42-520(a).

[348] Capitol Dispatch, Connecticut Enacts Protections to Shield Minors from Online Risks -Connecticut Senate Democrats, Sept. 30, 2024, https://www.senatedems.ct.gov/connecticut-enacts-protections-to-shield-minors-from-online-risks.

[349] *Id*.

[350] *Id*.

[351] Capitol Dispatch, *supra* note.

[352] FTC, Press Release, FTC Finalizes Changes to Children's Privacy Rule Limiting Companies' Ability to Monetize

Tech lobbyist groups are challenging some of these state laws designed to protect minors under the First Amendment.[353] Nonetheless, the provisions requiring opt-in consent for targeted advertising have not been struck down under First Amendment grounds.

B. Opt-Out of Profiling

Curbing behavioral advertising would diminish some firms' incentives to profile. But other firms would continue to profile when manipulating behavior increases profits. For example, gambling apps would likely continue profiling to induce customers to gamble more. Political candidates would continue profiling voters to induce them to either vote for them (or refrain from voting). So, the demand for profiling would exist without behavioral advertising.

Thus, the states should make three changes to their privacy laws for profiling. First, residents should be able to opt out of automated profiling even when the AI model relies only on publicly available data. As with behavioral advertising, when firms use AI in whole or in part to profile individuals, the distinctions among publicly available, sensitive, and non-sensitive personal data break down, when AI can infer sensitive information from publicly available data.

Second, residents should be able to opt out of automated profiling even when humans were involved. Profiling should be defined broadly, as it is in 13 states, to encompass any form of automated processing performed on personal data, including publicly available data, to evaluate, analyze or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location or movements.[354]

Third, states should allow their residents to opt out of automated profiling generally, rather than simply for "decisions that produce legal or similarly significant effects concerning the consumer."[355] This qualifier leaves too much to the firms' subjective discretion and does not protect residents from some of the principal harms from profiling, such as devising better ways to manipulate behavior.

Kids' Data (Jan. 16, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-changes-childrens-privacy-rule-limiting-companies-ability-monetize-kids-data.

[353] https://www.venable.com/insights/publications/2025/03/laws-regulating-minors-access-to-social-media

[354] Conn. Gen. Stat. Ann. § 42-515(30); see also Cal. Civ. Code § 1798.140(z); CO Revised Statutes § 6-1-1303(20); Del. Code Ann. tit. 6, § 12D-102(25); Ky. Rev. Stat. Ann. § 367.3611(23); Md. Code Ann., Com. Law § 14-4701(aa); Minn. Stat. Ann. § 325M.11(s); Mont. Code Ann. § 30-14-2802(19); N.H. Rev. Stat. Ann. § 507-H:1(XXIII); N.J. Stat. Ann. § 56:8-166.4; Or. Rev. Stat. Ann. § 646A.570(16); R.I. Gen. Laws Ann. § 6-48.1-2(21); Va. Code § 59.1-571.

[355] See notes **, *supra*.

C. Require Companies to Limit the Likelihood of the AI Models Re-identifying Data

Companies can obtain a competitive advantage by not having to comply with state privacy laws, including the time and compliance expenses associated with them.

Companies that use de-identified data should not be able to circumvent the privacy law when there is a reasonable probability that their AI can re-identify the data. Some states require controllers in possession of de-identified data to "[t]ake reasonable measures to ensure that the data cannot be associated with an individual,"[356] and "publicly commit to maintaining and using de-identified data without attempting to re-identify the data."[357] But enforcing these provisions will be difficult. Thus, when an AI model processes personal data, even de-identified data, the assumption should be that the privacy law applies unless the company certifies that it has taken specific steps to prevent re-identification. The onus should be on the company to establish the unlikelihood of re-identification.

D. Learning through the Data Processing Risk Assessments

Some states require companies to undertake data processing risk assessments when they process sensitive data or any personal data for purposes of behavioral advertising and profiling when

> *the profiling presents a reasonably foreseeable risk of: (A) Unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (B) Financial, physical, or reputational injury to consumers; (C) A physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where the intrusion would be offensive to a reasonable person; or (D) Other substantial injury to consumers.*[358]

For the statute's reporting requirements, data processing presents a heightened risk of harm to individuals when it involves, inter alia,

> *(1) the processing of personal data for the purposes of targeted advertising; (2) the sale of personal data; (3) the processing of personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of (A) unfair or deceptive treatment of, or unlawful disparate impact on, consumers, (B) financial, physical or reputational injury to consumers, (C) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person, or (D)*

---

[356] Conn. Gen. Stat. Ann. § 42-523(a)(1).

[357] *Id*.

[358] Tenn. Code Ann. § 47-18-3206; see also Del. Code Ann. tit. 6, § 12D-108; Conn. Gen. Stat. Ann. § 42-522(a); Md. Code Ann., Com. Law § 14–4710; N.H. Rev. Stat. Ann. § 507-H:8(1)(c); Va. Code Ann. § 59.1-580(a)(3).

other substantial injury to consumers; and (4) the processing of sensitive data.[359]

In its data protection assessment, the company must "identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks."[360]

These assessments are typically made available only to the state attorney general and remain confidential otherwise.[361] It will be interesting to see how candid these assessments are, especially when the firm knows that the prosecuting authority can access them. The risk assessments can be generic and broad, like the disclosures of risks in some SEC filings. (One reading Alphabet's risk disclosures in its 10-Ks over the past decade, for example, would never guess that the company monopolized multiple markets around the world.[362])

To be informative, this reporting requirement must actually capture the risks that the company perceives internally or that were brought to the company's attention and the law must deter, rather than promote, willful ignorance. In the infamous Facebook Files, *The Wall Street Journal* reported that Meta had internally recognized many serious risks posed by its social media platforms to teenagers and democracies.[363] Would Meta be as candid in reporting these risks under the state laws?

Accountability will largely come from the state attorneys general.[364] So, the usefulness of these data protection assessments will depend on the extent to which (1) at least one state attorney general presses the company on its disclosures (to ensure they reflect, at a minimum, risks that the

---

[359] Conn. Gen. Stat. Ann. § 42-522.

[360] *Id*.

[361] Tenn. Code Ann. § 47-18-3206.

[362] *See, e.g.*, Alphabet Form 10-K, for the fiscal year ended Dec. 31, 2024, at 11, https://abc.xyz/assets/77/51/9841ad5c4fbe85b4440c47a4df8d/goog-10-k-2024.pdf (citing as second risk factor: "We face intense competition. If we do not continue to innovate and provide products and services that are useful to users, customers, and other partners, we may not remain competitive, which could harm our business, financial condition, and operating results.").

[363] *The Facebook Files*, WALL ST. J., https://www.wsj.com/articles/the-facebook-files-11631713039.

[364] Except California, none of the state privacy laws provide a private cause of action. In California, the cause of action is limited. Californians can only sue firms if their personal information was "nonencrypted and nonredacted" or if the firm used their email address in combination with a password or security question and answer that would permit access to the account, and there was an "unauthorized access and exfiltration, theft, or disclosure [of their personal information] as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices." Cal. Civ. Code § 1798.150. Moreover, in some states, a company's violation of the privacy law cannot be the basis of a private cause of action (e.g., negligence action). *See, e.g.*, Cal. Civ. Code § 1798.150(c) ("Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law"); Conn. Gen. Stat. Ann. § 42-525(d); Tenn. Code Ann. § 47–18–3212(e) ("A violation of this part shall not serve as the basis for, or be subject to, a private right of action, including a class action lawsuit, under this part or other law.")

company perceives (or should have reasonably perceived) internally or that were brought to the company's attention), and (2) the other states can access the company's assessments to each state to ensure that the company is as forthright for each state. Since no state will likely have sufficient resources to unilaterally monitor these ecosystems that operate across the US and world, states should ensure that their privacy laws enable their attorneys general to coordinate with each other and share assessments (while keeping them otherwise confidential).[365]

CONCLUSION

Competition is often a far better discipliner of market behavior than command-and-control privacy dictates. But for competition to work (i.e., a race to the top rather than the bottom), the market participants' incentives must be aligned with our interests. By allowing residents to opt out of AI profiling and requiring them to opt into targeted advertising, the states can help better align incentives. These legislative changes will not address all the privacy concerns involving AI. However, by aligning incentives, policymakers can now rely on market forces to curb profiling and behavioral advertising, thereby limiting the risks they pose to our privacy, autonomy, well-being, national security, and democracy. Particularly considering the current congressional ineptitude, competition is a better option.

[365] For example, it is unclear under Tennessee's privacy law whether other state attorneys general or federal government can access these assessments. Tenn. Code Ann. § 47-18-3206(c) (providing that "attorney general and reporter" may request pursuant to a civil investigative demand that a controller disclose a data protection assessment that is relevant to an investigation conducted by the attorney general and reporter, and "[d]ata protection assessments are confidential and not open to public inspection and copying"). The other states and federal government can argue that they have the right to subpoena these reports, as they are not the public, and they will keep the reports confidential. But the company can argue that the statute contemplates that only the Tennessee attorney general can access its data protection assessments, which are otherwise intended to remain confidential.

References

Acemoglu, D., & Johnson, S. (2023). *Power and Progress: Our Thousand-Year Struggle Over Technology and Prosperity*. PublicAffairs.

Acemoglu, D., & Restrepo, P. (2020). Robots and jobs: Evidence from US labor markets. *Journal of Political Economy*, 128(6), 2188–2244.

Autor, D. H. (2023). *Labor Markets and Generative AI*. [Presentation/Testimony].

Autor, D. H., Dorn, D., Hanson, G. H., Pisano, G., & Shu, P. (2020). Foreign Competition and Domestic Innovation: Evidence from U.S. Patents. *American Economic Review: Insights*, 2(3), 357–374.

Bessen, J. E. (2020). *AI and Jobs: The Role of Demand*. NBER Working Paper No. 24235. https://doi.org/10.3386/w24235

Brandeis, L. D. (1913). *The Curse of Bigness*. [Essay; republished in various forms].

Capitol Dispatch. (2024, September 30). *Connecticut Enacts Protections to Shield Minors from Online Risks*. Connecticut Senate Democrats. https://www.senatedems.ct.gov/connecticut-enacts-protections-to-shield-minors-from-online-risks

Coyle, D., Diepeveen, S., & Wdowin, J. (2020). *Understanding the Economic Impact of Artificial Intelligence*. Bennett Institute for Public Policy.

Crawford, K. (2021). *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. Yale University Press.

European Commission. (2021). *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

Ezrachi, A., & Stucke, M. E. (2016). *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy*. Harvard University Press.

Federal Trade Commission. (2024). *Commercial Surveillance and Data Practices*. https://www.ftc.gov/reports/commercial-surveillance-data-practices-report

Ghosh, S. (2023). *Antitrust and Data Privacy in the Age of AI*. [Unpublished/Working Paper].

Lanier, J. (2013). *Who Owns the Future?* Simon & Schuster.

OECD. (2019). *Artificial Intelligence in Society*. OECD Publishing.

O'Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown Publishing.

Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press.

President's Council of Economic Advisers. (2016). *Big Data and Differential Pricing*. Executive Office of the President.

Stucke, M. E. (2018). Should We Be Concerned About Data-Opolies? *Georgetown Law Technology Review*, 2(2), 275–324.

Stucke, M. E., & Ezrachi, A. (2022). *How Big-Tech Barons Smash Innovation—and How to Strike Back*. Harper Business.

U.S. Department of Justice & Federal Trade Commission. (2023). *Merger Guidelines*. https://www.justice.gov/atr/2023-merger-guidelines

Varian, H. R. (2010). Computer mediated transactions. *American Economic Review*, 100(2), 1–10.

White House Office of Science and Technology Policy. (2022). *Blueprint for an AI Bill of Rights*. https://www.whitehouse.gov/ostp/ai-bill-of-rights

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.