Behavioral Target Should Be Allowed Or Not

Posted on October 2, 2018

Introduction

Behavioral targeting is the practice of selecting advertisements, recommendations, or messages according to information about a person's activities, interests, inferred preferences, location, device, purchases, or interactions. Online advertising systems may observe pages viewed, searches, clicks, app use, and responses to earlier advertisements. They then place users into categories or predict which message is most likely to attract attention. The original essay argues that behavioral targeting should be allowed because it can make advertising relevant and reduce wasted marketing. That position remains defensible only with conditions. Behavioral advertising can support free digital content, help businesses reach likely customers, and reduce exposure to completely irrelevant promotions. It can also create surveillance, manipulation, discrimination, security risk, and loss of control when data are collected across contexts without meaningful awareness. Behavioral targeting should therefore be permitted for adults when it is transparent, proportionate, secure, and subject to easy choice, but certain practices—especially targeting children, using sensitive data without explicit consent, or exploiting vulnerability—should be prohibited.

How Behavioral Targeting Works

A website or app may collect first-party information about what a user does within that service. Advertisers and technology companies may also share identifiers across numerous sites and apps, creating cross-context profiles. Cookies, mobile advertising IDs, pixels, software-development kits, account logins, location signals, and data-broker records can contribute to these profiles. Machine-learning systems then estimate interests or likelihood of action. A person who reads several pages about running may receive athletic-shoe advertising. A user who visits travel sites may see hotel promotions. The process can be useful when it reflects a current interest, but the same infrastructure can infer health concerns, financial stress, religion, political views, sexuality, or family circumstances. The ethical issue depends not simply on whether an advertisement is relevant but on how the information was obtained, combined, and used.

Contextual and Behavioral Advertising

Contextual advertising selects a message according to the content currently being viewed. A camera advertisement on a photography article does not necessarily require a long-term profile. Behavioral advertising uses information about the user's activity over time or across services. The distinction matters because contextual advertising can provide relevance with less surveillance. Businesses should consider whether profiling is actually necessary. If the same commercial objective can be achieved through page context, broad geography, or voluntarily stated preferences, extensive tracking may be disproportionate. Privacy-protective design begins by minimizing data rather than collecting everything and promising to secure it later.

Benefits for Consumers

Relevant advertising can help users discover products, events, jobs, or services that match current needs. It may reduce the volume of random promotions and allow a small business to communicate with a specialized audience. Recommendation systems can also improve navigation when users face large amounts of content. Some people willingly exchange data for personalization, particularly when the relationship is clear and the service offers genuine value. Behavioral data can help advertisers limit repeated exposure and measure whether campaigns reach intended audiences. These benefits should be recognized rather than assuming that every personalized message is harmful.

Benefits for Businesses and Publishers

Behavioral targeting can make marketing more efficient by directing limited advertising budgets toward people more likely to respond. This can help new or niche businesses compete with large brands. Publishers may earn revenue that supports journalism, entertainment, communication, and free online tools. Advertisers can compare creative material, frequency, and conversion in order to improve campaigns. However, these benefits are often claimed without disclosing how revenue is distributed among publishers, platforms, data brokers, and intermediaries. Efficiency for the advertiser does not automatically justify every method of collection. A business model should not receive immunity from privacy and consumer-protection standards merely because it funds free access.

The Problem of Invisible Surveillance

Many users do not understand how many parties receive data when they open a page or use an app. Privacy policies can be long, vague, and difficult to compare. Consent banners may use dark patterns that make acceptance prominent while hiding rejection behind several screens. This weakens the claim that users voluntarily agreed. Information collected in one context can also be used in another. A person may search for medical information to understand a relative's condition and later be categorized as having the illness. Contextual integrity, a concept developed by Helen Nissenbaum, emphasizes that privacy depends on whether information flows are appropriate to the social context in which data were provided. Behavioral targeting becomes intrusive when it violates those expectations. (Nissenbaum, 2010)

Profiling and Inaccurate Inferences

Advertising profiles are predictions, not verified descriptions of identity. They can be wrong because devices are shared, interests are temporary, data are incomplete, or algorithms mistake correlation for meaning. An inaccurate profile may repeatedly expose a person to distressing or inappropriate material. A correct inference can also be harmful if it reveals something private to family members or coworkers using the same device. People should have the ability to see and correct significant profile information where practical. Advertisers should not present inferred categories as objective truths.

Sensitive Personal Information

Health, precise location, financial circumstances, biometric information, race, religion, sexual orientation, immigration status, and intimate life require stronger protection. Targeting based on such data can expose vulnerability or discrimination. A person researching debt relief may be shown high-cost lending; someone experiencing grief may receive manipulative spiritual or commercial claims. The California Privacy Rights Act gives consumers a right to limit certain uses of sensitive personal information and a right to opt out of sharing for cross-context behavioral advertising. Legal definitions and exceptions are complex, but the ethical principle is clear: sensitive data should not be used for targeting merely because technology makes it possible.

Children and Adolescents

Children have limited ability to recognize persuasion, understand data collection, or resist design intended to prolong engagement. Behavioral advertising to children can exploit developmental vulnerability and encourage materialism, unhealthy food consumption, gambling-like activity, or risky products. U.S. federal law provides protections for online collection from children under thirteen through the Children’s Online Privacy Protection Act, while California imposes additional requirements and opt-in rules for the sale or sharing of information for users under sixteen in covered circumstances. Age assurance itself can create privacy risk if services demand identity documents from everyone. Platforms should use privacy-protective age-appropriate design and avoid behavioral advertising to minors rather than seeking technical loopholes.

Discrimination and Exclusion

Advertising systems can influence who sees housing, employment, credit, education, and healthcare opportunities. If a platform allows advertisers to exclude groups or uses historical response data to optimize delivery, protected populations may receive fewer opportunities even when the advertiser did not explicitly request discrimination. The harm differs from an ordinary product recommendation because access to essential opportunities affects equality. High-impact advertising should be subject to auditing, anti-discrimination rules, and limits on sensitive proxies. An algorithm should not be permitted to reproduce exclusion that would be illegal if performed directly by a human decision-maker.

Political Advertising and Manipulation

Behavioral targeting becomes especially sensitive in political communication. Microtargeted messages can be tailored to fears, grievances, or identity while remaining invisible to the wider public. Different groups may receive contradictory claims, making democratic accountability difficult. Targeting can help campaigns mobilize supporters and communicate relevant local issues, but voters need transparency about who paid, which audience was selected, and why they received the message. Public archives of political advertisements and targeting criteria can support scrutiny. Sensitive psychological or personal data should not be used to exploit vulnerable voters.

Frequency, Autonomy, and Persuasive Design

Advertising is designed to influence, but influence becomes manipulative when it undermines informed choice through deception, pressure, or exploitation. Repeated advertisements can create annoyance or the feeling of being followed. Platforms should use frequency limits and allow users to hide or explain recommendations. “Why am I seeing this?” tools should provide meaningful information rather than generic statements. Autonomy is strengthened when people can adjust interests, disable categories, and choose contextual rather than cross-site personalization.

Data Security

Large advertising profiles attract criminals, stalkers, fraudulent marketers, and hostile actors. Even information that appears harmless can become sensitive when combined. Companies should collect less, separate identifiers, encrypt data, limit employee access, set retention periods, and evaluate vendors. A company cannot promise that data are anonymous without assessing whether records can be reidentified. When information is no longer needed for the stated advertising purpose, it should be deleted. Security is a necessary condition for targeting but does not by itself make the collection legitimate. (Turow et al., 2015)

California Privacy Rights

California’s Consumer Privacy Act, as amended by the California Privacy Rights Act, gives covered consumers rights to know, delete, correct, and limit certain data practices. It also provides the right to opt out of the sale of personal information and the sharing of personal information for cross-context behavioral advertising. Covered businesses must provide a “Do Not Sell or Share My Personal

Information” mechanism and honor applicable opt-out preference signals. The law also prohibits discrimination against consumers for exercising privacy rights, subject to defined exceptions. These rights establish a baseline, but exercising them can still be burdensome. Ethical businesses should make privacy controls easier than the minimum required. (Acquisti et al., 2016; California Department of Justice, 2026; California Privacy Protection Agency, 2026)

Opt-In Versus Opt-Out

An opt-out system allows targeting until the user refuses, while opt-in requires affirmative agreement first. Opt-in provides stronger control but can create consent fatigue when every service presents repeated requests. Opt-out is less disruptive to advertising but depends on users understanding a hidden system. A balanced approach can vary by risk: contextual advertising and limited first-party personalization may operate with clear notice and easy opt-out, while sensitive data, cross-context tracking, and targeting of minors should require stronger consent or be prohibited. Consent should be specific, reversible, and independent of unrelated service access whenever possible.

First-Party Personalization

A user may reasonably expect a streaming service to recommend similar content based on viewing within that service. This first-party relationship is more transparent than a network tracking the user across unrelated websites. It still requires limits. A platform should explain the recommendation process, avoid sensitive exploitation, protect account data, and permit users to reset history. First-party data should not automatically be shared with third parties merely because a privacy policy contains broad language. The closer the use remains to the original context, the more defensible it generally becomes.

Cross-Context Behavioral Advertising

Cross-context advertising creates profiles from activity across different businesses, which increases the possibility of unexpected inference and misuse. It should therefore be subject to strict data minimization, clear identification of parties, opt-out signals, and prohibition of dark patterns. Advertisers should know which data sources support their campaigns and should avoid intermediaries that cannot document lawful collection. A company remains ethically responsible when it purchases targeting access rather than collecting the data itself. Outsourcing surveillance does not outsource accountability.

Measurement Without Individual Tracking

Advertisers need to know whether campaigns work, but measurement can use aggregated, delayed, or privacy-preserving methods. Randomized experiments, contextual comparison, on-device processing, clean rooms with strong governance, and conversion reporting with thresholds can reduce exposure of individual behavior. These techniques also have limitations and can be presented as private while retaining significant tracking. Independent evaluation and clear technical documentation are necessary. The objective should be sufficient measurement rather than perfect knowledge of each person.

Should Behavioral Targeting Be Allowed?

Behavioral targeting should be allowed only within defined boundaries. Adults may choose relevant personalization, and businesses have a legitimate interest in reaching potential customers. The practice becomes unacceptable when consent is deceptive, collection is excessive, sensitive conditions are exploited, minors are profiled, high-impact opportunities are discriminatorily distributed, or users cannot easily leave the system. Regulation should distinguish low-risk recommendation from cross-context surveillance. Enforcement should focus on actual data flows and design rather than on whether a company uses the word "personalization."

Recommended Safeguards

Organizations using behavioral targeting should publish concise notices, collect only necessary data, provide meaningful opt-out and deletion tools, honor universal preference signals, and prevent retaliation against users who refuse. Sensitive targeting and behavioral advertising to children should be prohibited or subject to strict affirmative consent where law permits. Platforms should audit housing, employment, credit, and political advertising for discrimination and manipulation. Data brokers and vendors should be contractually and technically monitored. Retention periods, security controls, and independent compliance review should be documented. Users should be able to understand why an advertisement appeared and correct or reset inferred interests.

Conclusion

Behavioral targeting can make advertising more relevant and help businesses and publishers use limited resources efficiently. Those benefits do not justify unlimited surveillance. Profiles can reveal sensitive information, make inaccurate inferences, exclude people from opportunities, manipulate vulnerable users, and create security risk. The practice should therefore be conditionally allowed rather than universally accepted or completely prohibited. Contextual advertising and transparent first-party personalization are generally less intrusive. Cross-context behavioral advertising requires strong choice, data minimization, and oversight, while targeting children or exploiting sensitive information should face strict limits. A sustainable advertising system must treat privacy and autonomy as design requirements, not as obstacles to be overcome.

References

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature, 54*(2), 442–492. https://doi.org/10.1257/jel.54.2.442

California Department of Justice. (2026). *California Consumer Privacy Act*. https://oag.ca.gov/privacy/ccpa

California Privacy Protection Agency. (2026). *Rights under the California Consumer Privacy Act*. https://privacy.ca.gov/

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Turow, J., Hennessy, M., & Draper, N. (2015). *The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation*. Annenberg School for Communication, University of Pennsylvania.