

Should Behavioral Targeting Be Allowed or Not?

Posted on October 2, 2018

View this essay online:

<https://academic-master.com/behavioral-target-should-be-allowed-or-not/>

Introduction

Behavioral targeting selects advertisements or recommendations according to information about a person's activities, interests, inferred preferences, purchases, device, location, or interactions. The practice can make marketing more relevant and help businesses reach audiences efficiently, but it can also create invisible surveillance when companies combine information across unrelated services. The central policy question is therefore not whether personalization is inherently acceptable or inherently harmful. It is whether the data collection and use remain proportionate to the commercial purpose, understandable to the consumer, secure, and subject to meaningful control. Contextual advertising, which responds to the content currently being viewed, can often provide relevance without long-term profiling, while cross-context behavioral advertising creates more significant privacy concerns because it follows activity across websites or apps. California law illustrates this distinction by treating certain cross-context behavioral advertising as "sharing" of personal information and giving covered consumers the right to opt out (California Department of Justice, 2026). A sustainable approach should distinguish low-risk personalization from practices involving sensitive data, minors, discrimination, or opaque third-party tracking.

Commercial Value and the Limits of Relevance

Behavioral targeting can create real benefits for consumers, publishers, and advertisers when it is based on an understandable relationship. A person researching running equipment may appreciate advertisements for shoes or local races, while a niche business can use limited advertising funds more effectively by reaching people who have shown an interest in its product category. Publishers may also depend on advertising revenue to support journalism, entertainment, communication tools, or other free services. These benefits, however, do not establish that every form of tracking is necessary. A recommendation based on activity within one service is generally easier for users to anticipate than a profile assembled from data brokers, mobile identifiers, pixels, location signals, and unrelated websites. The relevant test is whether extensive collection creates additional value that could not reasonably be achieved through contextual information, broad location, or preferences supplied voluntarily. Privacy protection is stronger when organizations minimize data at the design stage rather than collecting everything and relying on lengthy policies or security promises to justify

retention later (Acquisti et al., 2016).

Sensitive Data, Minors, and Unequal Effects

The risks of profiling increase sharply when advertising systems infer or use information about health, financial distress, precise location, religion, race, sexual orientation, immigration circumstances, or other intimate conditions. Such categories can expose a person to manipulation or reveal private information to others using the same device. Children and adolescents require particular protection because they may have less ability to recognize persuasive design, understand long-term data collection, or distinguish voluntary recommendations from commercially optimized engagement. Behavioral systems can also influence access to consequential opportunities when they determine who sees employment, housing, credit, or educational advertisements. Even when an advertiser does not directly exclude a protected group, automated delivery can reproduce historical patterns if systems optimize according to past response data. These concerns make accuracy only part of the problem: a perfectly accurate inference can still be intrusive or unfair. Ethical targeting therefore depends on the sensitivity of the data, the vulnerability of the audience, and the consequences of the advertisement rather than simply on whether a prediction is technically correct.

Transparency, Consent, and California Privacy Rights

Meaningful choice requires more than a privacy policy that few users can understand or a consent banner designed to make acceptance easier than refusal. California's Consumer Privacy Act, as amended, gives covered consumers rights that include access, deletion, correction, and an ability to opt out of the sale or sharing of personal information. The California Department of Justice explains that "sharing" includes cross-context behavioral advertising based on personal information derived from activity across numerous websites, and the state's 2026 rules require covered businesses to respond to qualifying opt-out preference signals in defined circumstances (California Department of Justice, 2026; California Privacy Protection Agency, 2026). These rules do not make every form of first-party personalization unlawful, nor do they eliminate the complexity of consent. They do establish a useful principle: consumers should have a practical method to refuse tracking that extends beyond the context in which they provided information. Controls are most credible when they are easy to locate, reversible, and expressed in language that describes actual data flows rather than vague promises of "better experiences."

Security, Accountability, and Privacy-Preserving

Alternatives

Advertising profiles can become valuable targets for criminals, fraudulent marketers, abusive partners, or unauthorized employees because seemingly ordinary information becomes sensitive when combined over time. Organizations should therefore limit retention, separate identifiers where possible, restrict internal access, encrypt data, review vendors, and delete information when the stated purpose has expired. Accountability also extends to purchased targeting access: an advertiser cannot avoid ethical responsibility merely because an intermediary assembled the profile. Measurement does not always require detailed individual tracking. Aggregated conversion reporting, contextual experiments, on-device processing, randomized tests, and privacy-preserving analysis can answer many campaign questions while exposing less personal information. These alternatives have limitations and should not be marketed as anonymous without technical evidence, but they demonstrate that advertising effectiveness does not require perfect knowledge of each person. Nissenbaum's concept of contextual integrity is useful here because privacy depends on whether information moves in ways that fit the context in which it was initially provided, not simply on whether a company obtained technical consent (Nissenbaum, 2010).

Conclusion

Behavioral targeting can support relevant advertising, product discovery, and publisher revenue, but its legitimacy depends on how information is collected, combined, and used. Contextual advertising and transparent first-party personalization usually create fewer privacy concerns because the connection between activity and recommendation is easier to understand. Cross-context profiling raises greater risks when consumers cannot see the parties involved, correct inferences, or leave the system without difficulty. The strongest safeguards are therefore data minimization, meaningful opt-out mechanisms, security, short retention, clear explanations, and additional restrictions for sensitive information, minors, and high-impact opportunities. California's privacy framework shows how law can distinguish cross-context behavioral advertising from ordinary first-party interaction while giving consumers specific rights over sale and sharing. The practical question is not whether all targeted advertising should be permitted or prohibited in one category. It is whether each use preserves enough transparency, proportionality, security, and consumer control to justify the data practices that make the targeting possible.

References

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature*, 54(2), 442-492.

California Department of Justice. (2026). *California Consumer Privacy Act*.

California Privacy Protection Agency. (2026). *CCPA statute and regulations effective January 1, 2026*.

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