



Mixed Signals

Many Companies May Be Ignoring Opt-Out Requests Under State Privacy Laws

BY
MATT SCHWARTZ, Policy Analyst (Consumer Reports)
AMBROSE VANNIER (2026), WILLIAM WALSH (2027), ALAN ZHANG (2027),
and SEBASTIAN ZIMMECK, Assistant Professor of Computer Science (Wesleyan University)

APRIL 1, 2025

Summary

Opt-out provisions, which allow consumers to restrict companies from selling or sharing their personal data for targeted advertising, are in many ways the core consumer protection under current state comprehensive privacy laws. However, opt-out provisions are meaningless if companies don't comply with them. Despite sending opt-out requests to 40 brand-name retailers, we were able to generate retargeted ads from 12 of them with relatively little effort. This corroborates previous research on the topic and strongly suggests that consumers' personal information may continue to be at risk for unwanted disclosure even when they take the appropriate steps to protect themselves under state privacy laws.

Introduction

On the surface, 2024 marked another watershed year for privacy legislation. According to the IAPP Westin Research Center, seven states passed comprehensive privacy laws—joining the seven states that passed a law in 2023. With the overall number of comprehensive state privacy laws now at 19, approximately 43 percent of the country's population lives in a state with such a law.

But while this is positive news in many ways, it is really only a portion of the story. Ultimately, what matters most is that privacy laws tangibly improve privacy outcomes for consumers. And this is by no means a foregone conclusion, nor is it easy to assess—state privacy laws are typically long and hard to parse, leaving plenty of room for businesses to violate the spirit of the law (if not the actual text) by taking advantage of loopholes or relying on the vagaries of the commercial data ecosystem to frustrate outsiders' efforts to assess their compliance. Perhaps because of these reasons, the implementation, enforcement, and outcomes of the state privacy laws have been fairly underexplored to date.

A key element of the types of privacy laws passed so far is the opt-out provision — which allows consumers to prevent companies from selling their data or using it for certain types of targeted advertising upon request. As previous Consumer Reports (CR) testing [showed](#), early state privacy laws tended to make this right incredibly difficult for consumers to use in practice by requiring them to opt out of unwanted data uses at each business individually (and using each business's different opt-out interface).

More recently enacted privacy laws typically include *universal opt-out provisions*, which allow consumers to signal to *all* companies in a single click that they don't want their data to be sold or used for targeted advertising. In theory, this should lead to widespread privacy benefits for the consumers who use such signals, while streamlining the compliance flow for businesses.

But what if companies are simply ignoring these requests? Previous CR testing showed that many companies [continued to share health-related data](#) even after receiving opt-out requests,

Mixed Signals: Many Companies May Be Ignoring Opt-Out Requests Under State Privacy Laws

while research from one of our co-authors [suggested](#) that the *vast majority* of companies were not reacting to universal opt-out signals like they are required to. Other recent research conducted by [two separate](#) privacy compliance companies similarly indicate that universal opt-out compliance is shockingly low.

If this is true, it would strike a major blow to the industry [narrative](#) that the privacy laws we have are sufficient and that we don't need more robust accountability mechanisms to ensure that the laws are obeyed. In our view, opt-out provisions are some of the most—if not *the* most—important provisions in current privacy laws since they are the main mechanism to stop the unwanted outward flow of personal data. Given our concerns, we decided to put these provisions to the test.

What we found alarmed us. Of the 40 retailers we tested, 12 (30 percent) appeared to serve us targeted ads on other websites despite our sending of [Global Privacy Control](#) (GPC) opt-out requests with every web request. In practical terms, this means that consumers' personal data may be sold or shared with third parties even when they've taken the appropriate steps to protect themselves.

Methodology and Limitations

Under many state privacy laws, covered companies have a legal obligation to honor opt-out requests—including opt-outs of sales and targeted advertising—sent by universal opt-out mechanisms, such as GPC (Consumer Reports and Wesleyan University are founding organizations and supporters of GPC). In practice, these mechanisms are implemented in privacy-friendly browsers, such as Brave and Firefox, or in browser add-ons, such as Optery and Privacy Badger, which users can install in their browsers to send opt-out signals. The very first public settlement under a state comprehensive privacy law came about after the California attorney general [alleged](#), among other things, that cosmetics retailer Sephora failed to treat GPC signals as a valid opt-out request.

[Many users find](#) online ad targeting creepy and invasive. It seems to imply that one's every click, page view, or interest is being collected, catalogued, and shared with wildly disparate entities across the internet ecosystem. A classic example is a pair of shoes, abandoned in an online shopping cart, that then follow the user around endlessly in advertisements as they browse the web.

Hypothetically, tools like GPC should address this concern, especially in states like [California](#) and [Colorado](#), where it has been officially blessed as a legally binding opt-out signal. With GPC enabled in those states, users shouldn't receive targeted ads for products they have viewed or attempted to purchase on other sites. If they do, it is highly suggestive that the business has either sold or shared their personal data for targeted advertising in contravention of the law.

Methodology

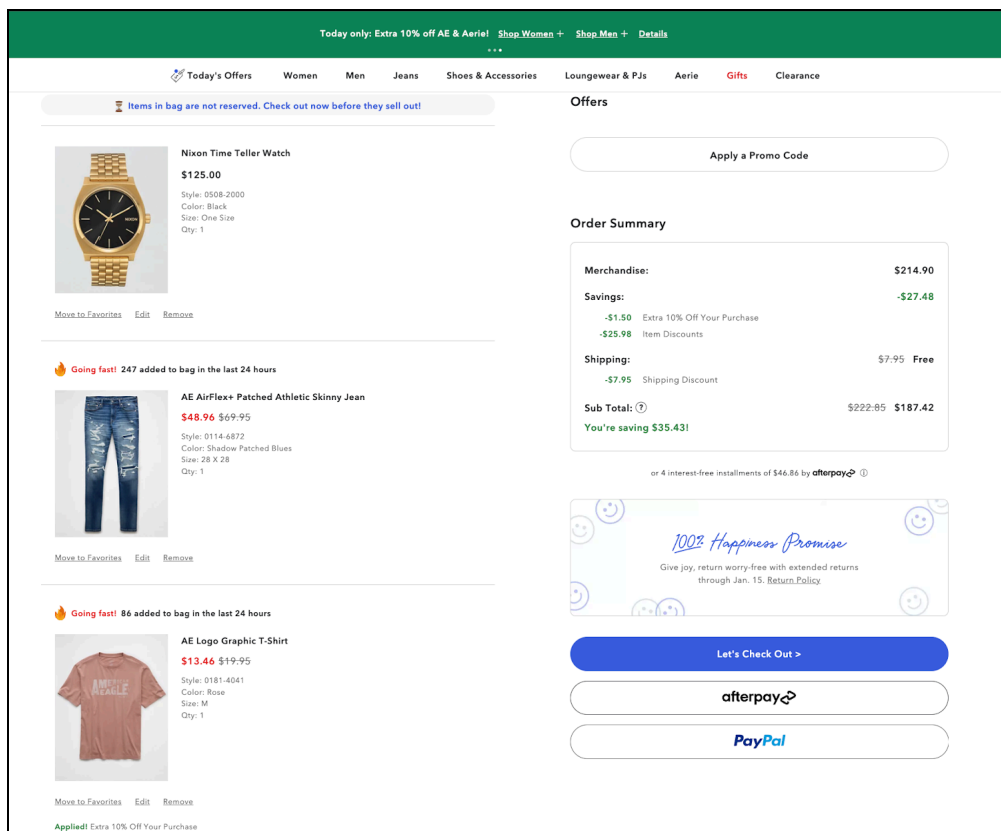
To test whether companies were really following through on their obligations, we used a variation of the methodology previously put to work in an earlier CR [article](#) about similar compliance issues after consumers had declined permission via cookie banners.

First, our four testers each downloaded the Mullvad VPN (virtual private network, a service that, among other things, allows users to change their IP address) and configured it to simulate our locations as either Los Angeles, Calif., or Denver, Colo. Then each tester created a brand-new Chrome account free of any previous browsing cookies that could muddy the results. We chose to test on Chrome because of its popularity (52 percent [market share](#) in the U.S.) and because it offers fewer default privacy protections than many other commonly known browsers, like Brave, Firefox, and Safari. Next, we installed the [Optery GPC Browser Plug-In](#) to send universal opt-out signals.

With our anonymous accounts configured, we moved to testing. To build our sample, we compiled a list of 40 retailer sites that we determined were likely to have to comply with the California or Colorado privacy laws based on disclosures in their privacy policies, website footers, or public information about their revenue. Our main criteria for inclusion on the list were that the company be big, well known to consumers, and likely to be the type of company that wanted to serve us targeted advertisements based on our activity on their site. The list comprised a wide variety of industries, including traditional retail (Macy's, Overstock, Wayfair), hospitality (Marriott), direct-to-consumer health (Hims), telecom (Verizon), and more. The full list can be viewed in the table below.

With GPC turned on, each tester visited 10 retailer websites, clicking through various product pages and placing two or three items per retailer site in their shopping carts, if possible. The idea was to simulate the experience of a consumer who had expressed interest in some purchases but never followed through. We thought that companies might wish to entice us via targeted ads to return to their website to complete the purchase.

Mixed Signals: Many Companies May Be Ignoring Opt-Out Requests Under State Privacy Laws



Our shopping cart at American Eagle.

Next, with GPC still turned on, each tester visited 10 publisher websites we selected based on their propensity to display targeted advertisements. The underlying content didn't matter much to us (we chose fairly general-purpose websites), as long as it was a fairly reputable publisher where major brands and advertising companies may want to spend money to advertise. These included sites like the Daily Mail, Huffington Post, and People Magazine. The full list can be viewed in the table.

Each tester visited each publisher website three times over the course of a week—once directly after filling their shopping carts at the retailer websites, once a few days later, and once at the end of the week—since we weren't sure how slowly or quickly any targeted ads may appear. We took screenshots of the advertisements the publisher websites served us and cross-referenced them against the list of retailers we had visited to determine whether any of the ads seemed to be retargeted based on our browsing history.

After a week, the testers wiped their Chrome browser accounts clean and tested a separate list of 10 retailer sites, following the same methodology described above. This allowed each tester to compare results with another tester in order to verify results.

Mixed Signals: Many Companies May Be Ignoring Opt-Out Requests Under State Privacy Laws

Table: Methodology Summary

	TESTER 1	TESTER 2	TESTER 3	TESTER 4
IP Location	California	California	Colorado	Colorado
Device Type	Desktop Mac	Desktop Mac	Desktop Mac	Desktop Mac
Browser	Chrome	Chrome	Chrome	Chrome
Retailer Sites Visited	<p>Round 1: Adobe, American Eagle, American Express, Anthropologie, AT&T, AutoZone, Home Depot, JCPenney, Overstock, and PetSmart</p> <p>Round 2: Article, Best Buy, Choice Hotels, CVS, Hims, Kohler, L.L.Bean, Ticketmaster, Pepsi, and Uniqlo.</p>	<p>Round 1: Article, Best Buy, Choice Hotels, CVS, Hims, Kohler, L.L.Bean, Ticketmaster, Pepsi, and Uniqlo.</p> <p>Round 2: Adobe, American Eagle, American Express, Anthropologie, AT&T, AutoZone, Home Depot, JCPenney, Overstock, and PetSmart</p>	<p>Round 1: Dollar Shave Club, GM, Grubhub, Ikea, Kohl's, Kroger, Marriott, Pottery Barn, Sephora, and Target</p> <p>Round 2: Ace Hardware, Ford, Macy's, Temu, Ulta, Verizon, Walmart, Wayfair, Wegovy, and Woman Within.</p>	<p>Round 1: Ace Hardware, Ford, Macy's, Temu, Ulta, Verizon, Walmart, Wayfair, Wegovy, and Woman Within.</p> <p>Round 2: Dollar Shave Club, GM, Grubhub, Ikea, Kohl's, Kroger, Marriott, Pottery Barn, Sephora, and Target</p>
Publisher Sites Visited	ClickHole, Daily Mail, Entertainment Weekly, Fox, Huffington Post, News, People Magazine, The Daily Beast, TMZ, Variety, and Weather.com	ClickHole, Daily Mail, Entertainment Weekly, Fox, Huffington Post, News, People Magazine, The Daily Beast, TMZ, Variety, and Weather.com	ClickHole, Daily Mail, Entertainment Weekly, Fox, Huffington Post, News, People Magazine, The Daily Beast, TMZ, Variety, and Weather.com	ClickHole, Daily Mail, Entertainment Weekly, Fox, Huffington Post, News, People Magazine, The Daily Beast, TMZ, Variety, and Weather.com

Findings

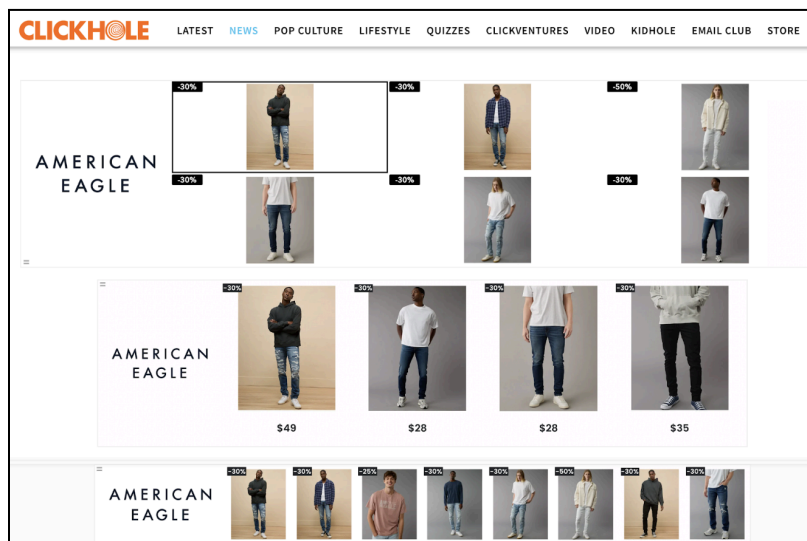
Of the 40 retailers we tested, 12 (30 percent) appeared to be serving us retargeted advertisements on other publisher websites despite our sending of GPC opt-out requests. We can break our sample of retailers into a few different tiers reflecting our level of confidence with the results: (1) surefire retargets, (2) very likely retargets, (3) sent ads, but unlikely to have retargeted us, and (4) no advertisements at all.

(1) Surefire Retargets

American Eagle (CA), Pottery Barn (CO), Ford (CO), Wayfair (CA), Woman Within (CO), JCPenney (CA), Macy's (CO), GM (CO), Uniqlo (CA)

We are almost certain that these retailers delivered advertisements to us based on our browsing activity, despite us sending GPC opt-out requests to them and the publishers that showed their ads. In these instances, we either observed advertisements that contained images of the exact items that we had viewed or placed in our shopping carts, or we found evidence from the AdChoices icon that the ad had been retargeted to us based on our browsing history. The AdChoices icon is a little blue triangle often found in the top corner of ads that is meant to provide additional information about why you received a particular advertisement.

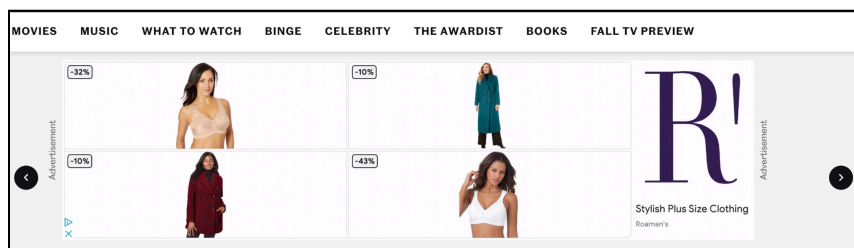
For instance, American Eagle flooded one tester with ads for a pair of distressed denim jeans and a distinctive American Eagle T-shirt that they had placed in their cart. When a second tester placed a pair of women's knit sweaters in their cart, they were similarly followed around multiple publisher websites with ads for those same items, along with numerous ads from American Eagle's intimate apparel and women's lifestyle sub-brand, Aerie.



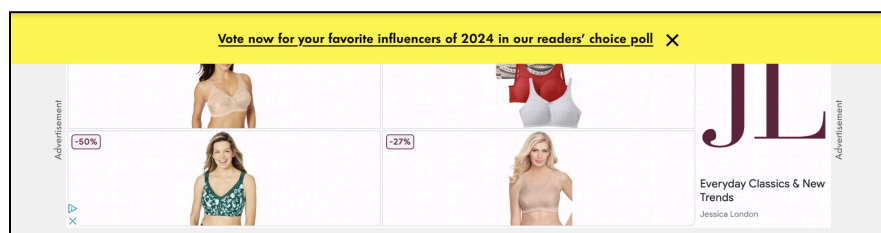
Several American Eagle ads containing the same T-shirt and jeans we had previously placed in our cart, seen on ClickHole.

Mixed Signals: Many Companies May Be Ignoring Opt-Out Requests Under State Privacy Laws

We saw similar behavior from the brand Woman Within and its parent company FullBeauty Brands which owns over a dozen similar brands. We were followed around by the same Glamorise Magic Lift Support Wireless Bra from our shopping cart, including by several affiliate brands that Woman Within had appeared to share our information with, including Roaman's and Jessica London.



Targeted ad seen at Entertainment Weekly for the same bra (top left) as placed in our cart at Woman Within, sold through the brand Roaman's.

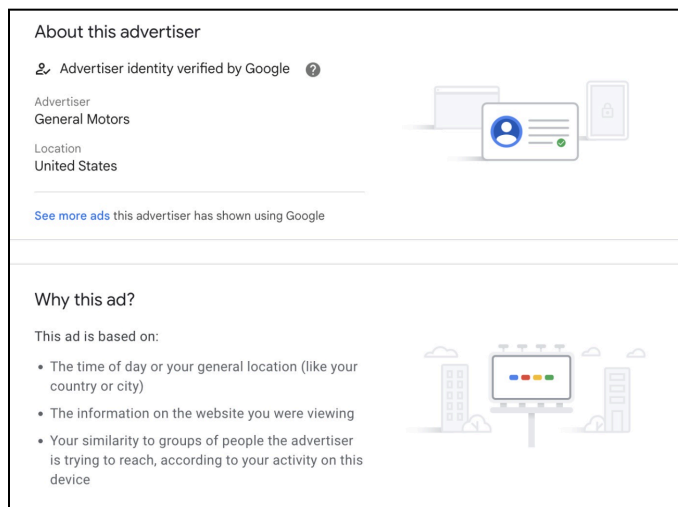


Targeted ad seen at People Magazine for the same bra (top left) as placed in our cart at Woman Within, sold through the brand Jessica London.

A matter of minutes after perusing several different vehicles, GM and Ford both sent us ads for similar vehicles — sometimes more than a dozen ads on the same page. (GM's ads appeared on just one publisher site, while Ford's appeared on multiple).



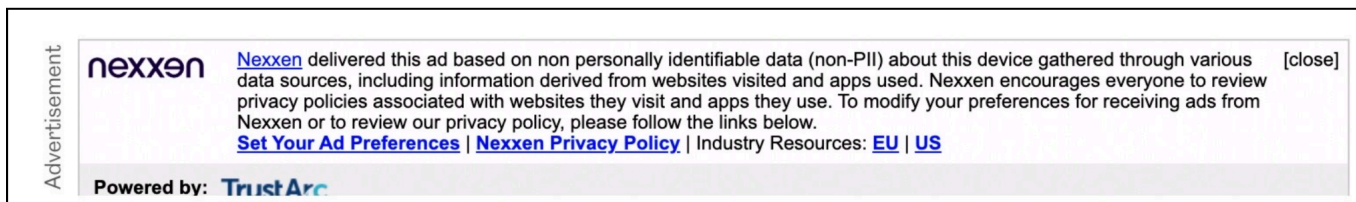
Targeted ad seen for the same 2024 Ford Bronco as viewed on Ford's website.



Advertisement from GM that was apparently based, in part, on "your activity on this device."

Mixed Signals: Many Companies May Be Ignoring Opt-Out Requests Under State Privacy Laws

And while the ads we received after visiting Pottery Barn did not exactly match the items we placed in our cart, we received advertisements that appeared to be based on information collected from our device, “including information derived from websites visited and apps used” (see below).



Result of clicking on the AdChoices icon on a Pottery Barn advertisement we received.

When we asked each of the companies in the “surefire” and the “very likely” tiers to explain why we might have received these targeted advertisements, we received the following responses (the remaining seven companies did not respond):

- GM referenced its privacy policy, which states that they “respond to the Global Privacy Control (GPC) signal when we detect that it is enabled on the particular web browser used to access our websites.”
- Ford said: “There could be a number of reasons this might be occurring, such as visiting a site with the Ford name that Ford does not control, such as a Ford dealer site or an unaffiliated accessories site.” (Note: We viewed Ford products only on Ford’s official website.)
- Wayfair said: “Our systems are set up to implement GPC signals in accordance with industry standards and regulatory requirements.”
- Pottery Barn asserted: “The advertising activity that you described is not meant to be controlled by GPC or by do not sell or share opt outs under applicable state privacy laws. GPC and those laws provide an opt out from advertising based on interactions with multiple websites, often called cross-context behavioral advertising.”
- Hims said: “Our site automatically opts Colorado users out of sharing collected information for non-essential purposes, including advertising. Further, we honor the privacy choices set by GPC signals for all non-essential purposes through a privacy compliance vendor.”

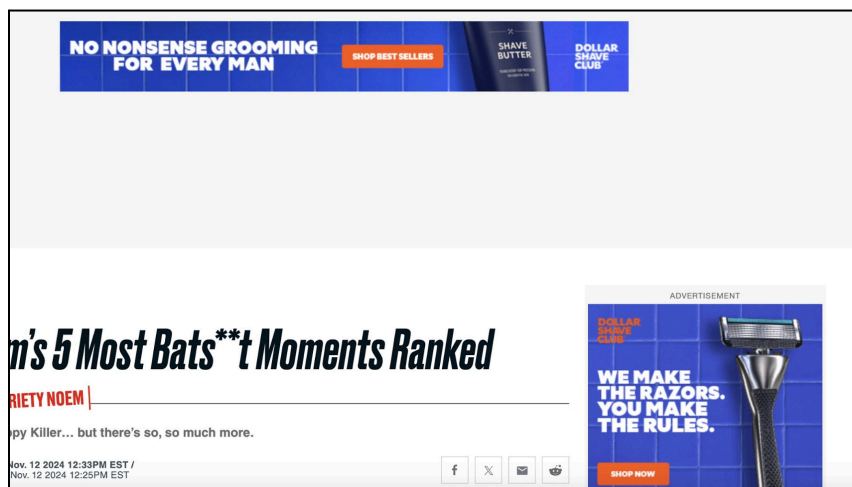
(2) Very Likely Retargets

Dollar Shave Club (CO), Kroger (CO), Hims (CO)

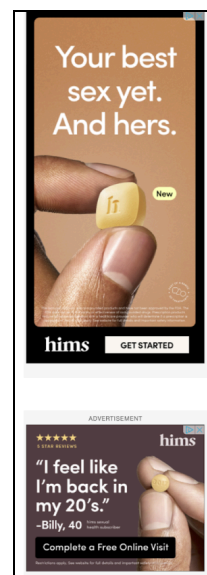
These websites all showed us advertisements we believe were sent on the basis of our web activity, but the ads tended to be more generic than the ones we received from businesses in the “surefire” tier, slightly lowering our confidence level overall.

Mixed Signals: Many Companies May Be Ignoring Opt-Out Requests Under State Privacy Laws

Dollar Shave Club and Hims are both direct-to-consumer companies that frequently leverage digital advertising to reach consumers. We received advertisements for both of their services mere minutes and just several clicks after visiting their websites and placing various items in our cart—which strongly suggests that the ads’ presence on our browsers was not a coincidence. The two testers that did not visit Dollar Shave Club and Hims did not receive ads for them. It was unclear from the content of the ads alone whether the advertisements were targeted based on our abandoned purchases or simply our visit to their website.

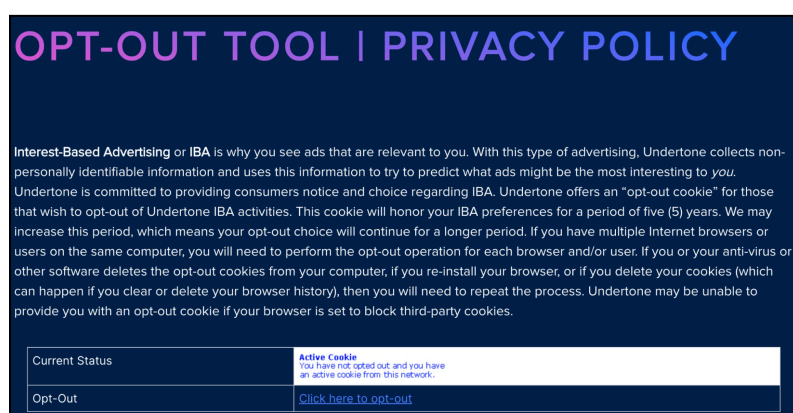


A pair of Dollar Shave Club ads we received on the Daily Beast.



Hims ads seen on Daily Beast.

King Soopers is a sub-brand of the grocery chain Kroger with locations in Colorado and Wyoming. King Soopers showed us ads across numerous publisher websites after we viewed several grocery items on its website. An AdChoices display indicated that at least one of the advertisements was placed because of cookies that an ad network used by Kroger had placed on our device.



King Soopers appeared to target us based on cookies; clicking on AdChoices revealed an “active cookie” for interest-based advertising.

(3) Sent Ads, but Unlikely to Have Retargeted Us

Temu, Sephora, Walmart, Target

This tier represents the list of websites for which we received advertisements but have no strong reason to believe they were retargeted to us based on our web activity. None of the advertisements from these companies contained items we had placed in our shopping carts. In some cases, testers who had not visited these websites received similar generic advertisements for these companies. Our best guess is that these were “contextual advertisements” that were placed on the basis of the content of the publisher sites we were visiting—or were simply part of large advertising campaigns that did not rely on individualized tracking for placement.

(4) No Ads at All

The remainder of our test sites did not display any advertisements on the publisher websites that we visited. Possible explanations include that these businesses were not engaged in digital marketing campaigns at the time of our testing, that these websites would have sent us targeted ads but appropriately respected our opt-out choices, or that we simply did not visit enough publishers to receive ads from these companies.

Limitations

While we intended to simulate the browsing experience of the average internet user in California or Colorado, there were some inherent limitations to our experimental design.

First, because we used a VPN to access the retailer sites, it is possible that they had some way of recognizing our out-of-state location—thus negating their legal obligation to respond to our opt-out requests. That said, IP addresses are a common way sites [verify location](#) for the purposes of privacy law compliance. Further, the type of sites we visited are not those known to parse for VPN (e.g., location-gated services, like Netflix). Also, many of the target sites automatically detected our ZIP code and offered us options for local pickup or shipping that suggested they were treating us as state residents.

Mixed Signals: Many Companies May Be Ignoring Opt-Out Requests Under State Privacy Laws

Order Summary (3)

This order qualifies for Free Shipping!

Item Subtotal (3)	\$954.88
Deliver to Denver - 80202 ▾	FREE
Retail Delivery Fee	\$0.29
Estimated Tax	\$84.12


Total **\$1,039.29**

You Save **\$715.01**

Earn \$47.74 in Rewards!

With 5% back¹ on every item, plus members-only sales, and more

[Join now for \\$29/year](#) | [Learn More](#)



[Proceed to Checkout](#)

Our shopping cart at Wayfair automatically inserted a ZIP code based on our IP address.

Second, in some instances, we couldn't be 100 percent certain that a given company was required to comply with the relevant state law since companies are generally not obligated to publicly affirm their compliance status. State privacy laws have sometimes nuanced compliance thresholds—for instance, under the Colorado Privacy Act (CPA), companies must comply if they “collect or process” the personal data of 100,000 state residents in a calendar year, *or* if they derive revenue from the sale of personal data *and* “process or control” the personal data for 25,000 or more state residents. We addressed these constraints by selecting especially large businesses very likely to surpass the coverage thresholds and confirming that their privacy policy included mention of providing consumer rights in the relevant state.

- **Right to Opt-Out of the Sale or Sharing of Personal Information:** You have the right to opt-out of the “sale” or “sharing” of your Personal Information, as such terms are defined in California privacy laws.

This means that, if you opt out, going forward, we will not sell or share your Personal Information with such third parties to use for their purposes, including cross-context behavioral advertising (as defined by California law), unless you later direct us to do so.

If you are a resident of Connecticut, Colorado, Utah, or Virginia, you may take advantage of certain privacy rights, such as to request access, correction, deletion, or a copy of your Personal Information. Because we may “sell” Personal Information as such term is defined in Connecticut and Colorado laws, or engage in “targeted advertising” as such term is defined in Connecticut, Colorado, Utah, and Virginia laws, you may also exercise your right to opt-out of such sales or targeted advertising where available. You have the right to appeal a denial of your privacy rights.

An screenshot from Dollar Shave Club's privacy policy providing rights to California and Colorado residents.

Mixed Signals: Many Companies May Be Ignoring Opt-Out Requests Under State Privacy Laws

Third, we visited only 10 publisher websites, and the average consumer likely visits many more over the course of a week. We limited our visits to publisher websites because we manually captured screenshots of the advertisements we received and collecting a larger sample would have required automation. However, as discussed in the Findings section, even with our small sample, retargeted ads appeared to populate publisher sites frequently—though it is possible that if we had visited more publisher sites, we would have seen even more retargeted ads.

Fourth, it is possible that the companies in Tiers 1 and 2 might have interpreted California or Colorado law to exclude their marketing campaigns from coverage of the targeted advertising opt-out. While defined slightly differently under both laws, “targeted advertising” is generally defined to include advertising based on personal data collected across nonaffiliated businesses. Regulated businesses have a history of [aggressively narrow](#) interpretations of state privacy law and may argue that [retargeting](#) is out-of-scope. For example, when reached for comment Pottery Barn stated: “[t]he activity you described ... sounds like retargeting based on interactions with just one website—potterybarn.com. That activity is expressly excluded from requiring a GPC opt out under Colorado law and is not the activity described by the GPC documentation.”

In our view, the targeted advertising we saw clearly did depend on personal data collected by at least two businesses (the retailer site, the publisher, and likely other ad-tech intermediaries that help to place ads on behalf of businesses) and is clearly subject to opt-outs under California or Colorado law. Moreover, such a reading is clearly inconsistent with the intent of state privacy laws. It is difficult to believe that regulators sought to exclude the canonical example of targeted advertising—shoes that follow you from site to site in the form of advertisements—from their definition of targeted advertising. Even if the behavior we observed were somehow out of the scope of the targeted advertising provisions, the businesses still may have impermissibly “sold” personal data to advertising partners in a similar way to that which was described in the California attorney general’s Sephora [complaint](#).

Finally, we note that our lists of retailer and publisher websites were not intended to represent the internet as a whole or be representative in some other way. As previously discussed, we intentionally selected for certain characteristics (e.g., size and propensity to send/display targeted ads) convenient for our research that may meaningfully differ from the broader subset of companies obligated to comply with state privacy laws. However, as further elaborated on in the Discussion section, we do believe our results are suggestive of a troubling trend worth further exploration.

Discussion

Our ability to generate retargeted ads on 12 of 40 of our test websites with just a few clicks suggests that there may be a major state privacy law compliance gap, corroborating [previous work](#) on this topic. Opt-out provisions aren’t a niche component of state privacy laws; they are in many ways the core consumer protection, as they function as gatekeepers for which information enters the ad ecosystem. They provide consumers with an actionable step to protect their data

Mixed Signals: Many Companies May Be Ignoring Opt-Out Requests Under State Privacy Laws

from flowing in unwanted directions and if businesses aren't complying with them, it makes one wonder how they are complying with the other requirements present in the law (e.g., access, correction, and deletion rights). Even more concerningly, the retailer sites we tested tended to be large and well resourced, meaning that they are ostensibly in a *better* position to comply with state privacy laws than smaller companies.

To be fair, this issue might extend beyond just the retailer sites themselves. Publishers weren't the main targets of our investigation, but they too have legal obligations that they often appeared not to be meeting by helping facilitate targeted advertisements after receiving opt-out requests. They, too, are bound to adhere to universal opt-out signals in California and Colorado by limiting the sale or use of personal information for targeting advertising. They might not be as proactively tracking consumers around the internet as retailers, but if they had held up their end of the privacy bargain, we wouldn't have seen as many targeted ads.

Moreover, while we only tested the California Consumer Privacy Act (CCPA) and CPA, there are 10 other state privacy laws with similar requirements to honor universal opt-outs, many of which come into effect at some point this year. Notably, [Connecticut](#) and [New Jersey](#) recently joined California and Colorado by explicitly mandating compliance with GPC signals (though New Jersey's requirement won't go into effect until July 15, 2025). If current trends hold, those states are likely to be joined by several others in the coming years. And while the CPA is a newer law, the CCPA has been in effect for several years now, providing ample time for the large companies that must comply with all state privacy laws to get up to speed with their compliance obligations. Universal opt-out requirements are now widespread, and the types of entities we tested should not be surprised about what the law says and requires from them to be compliant.

Of course, this report is also about more than just technical violations of a privacy law—there are real human stakes. Some of the sites we tested were collecting highly sensitive data that could cause serious harm to individuals if it were to make it into the wrong hands. For example, when we visited Hims, we sought out treatments for incredibly personal issues—erectile dysfunction and weight loss. The average person likely does not want this type of information to be revealed to others, which is why Hims touts its confidentiality-enhancing business practices so prominently in its marketing [materials](#). Yet the apparent sharing of personal data in contradiction of our opt-out requests means that data about one's activities on the site could easily make it into the hands of data brokers or even insurance companies that could ultimately use the information against consumers.

The relative ease with which we uncovered these issues also suggests that existing enforcement frameworks might not be sufficient to protect consumers from privacy violations. Due to extensive industry lobbying, every single comprehensive state privacy law passed so far provides exclusive enforcement authority to the state enforcers, saddling often overworked and underresourced government officials with oversight of these laws. If we were residents of the states where we found the suspected violations, our only recourse would have been to complain to regulators and hope that they followed up. If they declined to do so, there would be no other option.

Mixed Signals: Many Companies May Be Ignoring Opt-Out Requests Under State Privacy Laws

Leaving enforcement solely in the hands of state attorneys general emboldens companies to ignore the law because they know that their state attorney general is unlikely to have the time, money, or staff to investigate violations comprehensively. Notably, there have been only a handful of public enforcement actions under state privacy laws to date. Instead, CR has long argued that consumers who have been harmed by violations of the law should have the ability to take action to protect themselves via a private right of action. It seems like basic common sense that individuals should be able to hold companies accountable when the government decides that it cannot, but so far corporate interests have outweighed the public good in the minds of legislators.

Conclusion

While our findings are troubling, we are hopeful that they can kick off a new conversation about compliance and enforcement of state privacy laws that will improve protections for consumers overall.

In the meantime, Consumer Reports and our partners at the Electronic Privacy Information Center (EPIC) are working to raise the bar in state laws through our model [State Data Privacy Act](#). We'll continue our extensive state-by-state advocacy to ensure that consumers receive the protections in privacy laws that they truly deserve—and that those protections are honored once in place.

Sebastian Zimmeck received funding from the National Science Foundation (Award #2055196) for this research and is grateful for the support. Sebastian also thanks Wesleyan University, its department of mathematics and computer science, and the Anil Fernando Endowment for their additional support.