

“Surveillance pricing” and ways to avoid it

Jared Newman | February 17, 2026 | adviserator.com

“This price was set by an algorithm using your personal data.”

If you live in New York State, you might start noticing this disclaimer while shopping online. As [noted by Ronan Farrow](#), a state law that took effect late last year requires companies to disclose when they’ve used your data to decide how much they’ll charge you.

This practice, known as “surveillance pricing,” allows companies to set different prices based on factors like your location, device usage, income, and purchase history. The ostensible goal is to figure out how much you're willing to pay and possibly charge more than usual.

Surveillance pricing has been happening for years, and not just in New York. Some notable examples:

- In 2012, the Wall Street Journal found that Staples [used customers' location data to charge more through its website](#) if there weren't any competing office supply stores nearby.
- In 2019, the Minneapolis news station KARE caught Target [charging more through its app](#) when customers looked things up from inside a Target store, likely because customers were already motivated to buy at that point.
- In 2024, SFGate reporter Keith Spencer found that Expedia and Booking.com were [charging far more for the same hotel rooms](#) when the searches came from San Francisco-based IP addresses.
- Last year, a [Consumer Reports investigation](#) found that Instacart prices varied by up to 23% for different users shopping from the same exact grocery store. (Instacart called this an "experiment" and claims to have abandoned it.)
- Kroger also confirmed to Consumer Reports last year that it [uses demographic and behavioral data](#) to help decide which digital deals customers are eligible to get.

Meanwhile, AI threatens to make things worse. Last year, Delta had to clarify that it [isn't tweaking prices based on personal data](#), after partnering with an AI startup that boasted of [doing exactly that](#).

The New York State law doesn't ban surveillance pricing, but it'll at least reveals which companies are engaging in it. So far, customers have reported seeing the disclaimer in [Uber Eats](#), [Doordash](#), [Target](#), [Postmates](#), and the [Washington Post](#), and I'm sure that's just scratching the surface. If a companies are setting personalized prices in New York, they're probably doing it elsewhere without any disclosure.

What you can do about it

There's no foolproof way to avoid being charged more through surveillance pricing, and in some cases your personal data could lead to better deals. Not knowing one way or the other is part of what makes the practice so insidious.

Still, there are a handful of countermeasures you can at least consider:

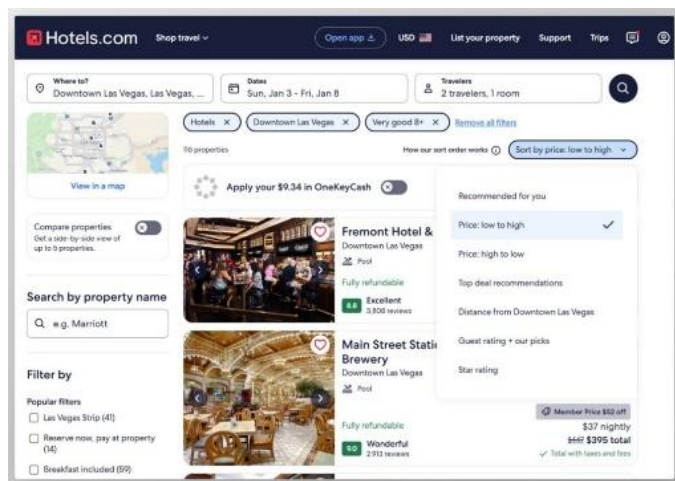
Shore up your privacy settings: My [post from a couple weeks ago](#) includes some simple steps to limit what companies collect and share about you. Pay particular attention to which apps have access to your location, as this information can be used against you (as in the Target example above).

Logged in vs. logged out: In the responses to Farrow's post, one person [reported](#) seeing higher prices for a United flight after logging in with their frequent flier number. While I'm not sure what the explanation was in that case, double-checking prices in an incognito or private browser tab can help determine whether your loyalty is being rewarded or punished.

Try different devices: Last year, Lifehacker's Jeff Somers found that a TCL TV from Amazon [cost \\$9 more on his phone](#) than it did on his computer. A quick check of your other devices could turn up better (or worse) prices.

I've seen suggestions to use a VPN as well, though I'm less inclined to suggest doing so just for shopping purposes. VPNs [have their own costs and complications](#), and retailers may be able to detect when you're using one. Somers found that using a VPN had no bearing on prices.

Bonus tip: Sort by price



Even if companies aren't charging different prices for the same exact items, they may promote more expensive options based on what they think you'll pay for. Orbitz, for instance, once [infamously put pricier hotels in Mac users' search results](#) compared to folks who searched on Windows PCs.

With that in mind, here's an oldie-but-goodie [from the Advisorator archives](#): Whenever you're shopping online, look for the option to sort by price from low to high, then use additional filters such as star rating or features to narrow things down. Don't trust the default "recommended" results, which might steer you toward pricier options. I can't tell you how many times I've found cheaper hotels and rental cars just by sorting the results.