

Siara (00:01)

Jacob in FIDI might end up paying more for laundry detergent than Jill in Midtown simply because of his data profile.

the FTC launched a formal study into what it called the surveillance pricing ecosystem.

Surveillance pricing is when a company uses personal data about you to help determine the

Price, that you receive.

The investigation found that some individual products varied as much as 23% in price.

One reported example involved a vacuum that appeared \$148 more expensive inside the store than outside.

Outside

of the store.

want to explain exactly what surveillance pricing is, who might be doing it, and what you can do to help protect yourself from it.

So I'm gonna give you

four ways that you can make yourself a little harder to profile.

Hey, happy Thursday. I have a lot of fascinating information for you today, some that surprised even me. So let's just get right into it.

I talk about data privacy a lot on the show, but also just a lot in my personal life, like at family functions, at happy hours, and I always run into the person who's kind of like, what does it matter, Siara Like they already have all of my data, they already have all of my information. If they have just one more data point, does it really matter? Like this person just doesn't really care as much about data privacy.

If you're that person, I get it. Protecting your data can feel very monotonous and it can feel very pointless at times. But I promise you, surveillance pricing is about to become your reason to care. Today I'm going to explain the frankly insidious pricing practices that corporations have been using. It has everything to do with you, specifically you, and your unique data profile.

We have all become somewhat accustomed to personalized advertising, right? Like if I Google running shoes, I fully expect a running shoe ad to follow me around the internet for like three weeks.

That said, one of the basic assumptions that we make as consumers is that when we walk into a store or open a website, there is one price for the thing that we want to buy. Maybe there is a sale, maybe prices went up that month, maybe Uber is expensive because everyone just left a concert. But we are all paying the same price for the same product or service at any given moment in time. Surveillance pricing violates that basic rule of commerce. Surveillance pricing is when a company uses personal data about you to help determine the

Price, discount, promotion, or offer that you receive. Meaning Jacob in FIDI might end up paying more for laundry detergent than Jill in Midtown simply because of his data profile. Are you okay with that? I'm not really feeling good about it, and the FTC is definitely not feeling good about it.

About two years ago in July of 2024, the FTC launched a formal study into what it called the surveillance pricing ecosystem. And Consumer Reports just dropped a report explaining how rideshare pricing algorithms can produce dramatically different fares for consumers requesting essentially the same rides. There are several major industries under scrutiny for these practices, so this is something worth paying attention to.

Today I want to explain exactly what surveillance pricing is, who might be doing it, and what you can do to help protect yourself from it. and also at the end of the episode, I'll share some interesting news about Comcast and some good news for consumers in New York. Alright, so here's what you need to know about surveillance pricing.

The first thing to understand is that dynamic pricing, which is something you're probably very familiar with, is very, very different from surveillance pricing. Dynamic pricing means that prices change because the circumstances around the transaction change. Uber gets more expensive when demand is high, flights get more expensive around Thanksgiving, a hotel room can cost \$200 one weekend and \$600 the next. The market conditions changed, so the price changed. That's just basic supply and demand, very normal. Surveillance price

Pricing adds information about the individual consumer to that equation. Your data can potentially become one of the inputs used to decide the price, the promotion, the discount, or even which products you are shown.

So that's another important distinction here. It's not always going to be that Jill paid \$13 for laundry detergent and Jacob paid \$18. It might be that Jill was shown the discount and Jacob wasn't. Or that Jacob was pitched the premium product and Jill was pitched the budget one. These retailers can determine who receives a coupon, how large the discount is, which offer you get, and which products get placed in front of you simply based on your data. But either way, Jacob is shelling out more money than Jill for.

That specific item.

Here's another example. If an algorithm knows that Jacob almost always buys the expensive version of something, they might show him the premium product first, which is not so crazy. It

also might only show Jill a coupon because they know that Jill will abandon her cart if she's not shown it at the checkout. It also might predict that Jill is extremely motivated to buy something right now, and there may be less of a reason to give her that same incentive. The FTC found that these systems can draw from incredibly granular information, including

Your precise location, your demographics, browsing history, shopping history, what channel you're shopping through, what you search for, what you leave sitting in your cart, and even your mouse movements on a web page.

This is where personalized advertising and personalized pricing start to kind of feel like cousins. We know that businesses have spent years developing technology for predicting what message is most likely to make you buy. Now some of that same data and segmentation can be applied to the actual transaction. The FTC has explicitly connected the sophisticated targeting capabilities developed in ad tech with the emerging ability to influence prices.

There's a concept called willingness to pay or WTP that's important to understand here. It's pretty self-explanatory. It's the highest price a customer is willing to spend on a good or service before they refuse to buy. It functions as a price ceiling for a specific consumer and helps businesses set a profitable price. Maybe Jacob's WTP for a laundry detergent is \$20, but Jill's is \$14. So the company sets the price at \$13 because it needs both of them as customers.

But as they get better at estimating each of our individual limits or our WTPs, they could theoretically charge Jacob closer to \$20 while still giving Jill the \$13 offer. And of course, AI and the massive amount of data collected about people online make that kind of prediction much easier to attempt at scale.

So, what companies are actually implementing surveillance pricing? I wish I had a clean list of 20 companies that have been caught doing this, but it's not quite that simple, unfortunately. This information is limited because the FTC has to protect confidential business information from the companies it investigated. What we do know is that there are confirmed industries where personalized or algorithmic pricing is already being tested or scrutinized. The grocery industry is probably the clearest place to start, and I feel like one of the most

Problematic. Consumer Reports spent months investigating Instacart and found that shoppers were being shown different prices for identical groceries from the same stores at the same time. Their testing included retailers such as Albertsons, Costco, Kroger, Safeway, Sprouts Farmers Markets, and Target. The investigation found that some individual products varied as much as 23% in price. Instacart confirmed that it was running pricing experiments for 10 retail partners, but

But

it did decline to publicly identify those 10 partners. Instacart also says that shoppers' personal information, such as demographics, their shopping behavior, supply and demand, were not used

to determine who received which price. So we can call this confirmed algorithmic pricing, but we cannot call that specific experiment confirmed surveillance pricing.

Consumer Reports also said that Instacart did acknowledge food brands can use behavioral data when testing discounts and promotional offers through its Eversight software.

So it's all a little bit blurry what Instacart and their partners are doing, but after the investigation and the backlash, Instacart ended the item price testing program in December of 2025. But it said that retail and food brand partners can still test promotions and discounts through the platform.

Consumer Report's investigation also found that location data alone can affect what a shopper sees. They cited that Target's app displayed different prices depending on whether a shopper's phone was physically inside the store or farther away. One reported example involved a car seat that appeared \$72 more expensive inside the store than outside of the store, and similarly a vacuum that appeared \$148 more expensive inside the store than outside.

Outside

of the store. Another industry under scrutiny for this is rideshare platforms.

Just this summer, Consumer Reports released a new investigation showing that people requesting essentially the same Uber and Lyft routes could receive substantially different fare offers, in some cases differing by close to 50%. Uber and Lyft both deny that these differences are a result of surveillance pricing, but Congress wants to know more, so they've demanded documents from Uber, Lyft, Bookings Holdings, Expedia, and Instacart to look more into it. While we can't confirm that any specific brands specifically engage in surveillance pricing,

Because the FTC can't share the names directly. The FTC can illustrate what this may look like in other instances, and they did. So a quote from the report is that a consumer who is profiled as a new parent may intentionally be shown higher-priced baby thermometers on the first page of their search results, which feels icky to me. Again, that's a hypothetical, but it's interesting.

Another interesting wrinkle in this situation is that there's an important middleman. Retailers themselves are not hiring machine learning engineers to create these complex psychological models of Jill and Jacob calculating their individual willingness to pay for their product lines. That would not be efficient, and the FTC knew this.

When the FTC launched this study, they went directly to the companies sitting behind the retailers that were providing pricing, analytics, consulting, and personalization technology. They went to MasterCard, JPMorgan Chase, Accenture, McKinsey, Pros, BloomReach, Revionics, and Task Software. These are what the FTC considers intermediaries.

the retailers actually hired these companies to provide algorithms that address what different groups or individuals are offered. The FTC found that the intermediaries collectively worked with at least 250 clients, including companies selling everything from groceries to apparel.

My immediate question when I heard some of those names was, are our bank selling us out? I'll be honest. But that's not necessarily the case because again, the FTC has to aggregate and anonymize the information because they need to protect trade secrets.

But what we do know is that these systems can, of course, pull from first-party data, meaning information the company collected directly from you, but also third-party data, meaning information obtained elsewhere. They can also use inferred data, which means an algorithm predicts something about you based on the information it already has. consumer reports found that Instacart had obtained personal data from Acxiom and Epsilon. These are two major data brokers. So what I'm inferring is that the surveillance pricing can be powered by the same

enormous data ecosystem that they use to target ads to us.

The retailer may have its own data, but they also may buy additional information. We know that sometimes people buy information off the dark web, meaning they buy data that hackers stole. So I'm super curious what's kind of powering all of the data behind surveillance pricing. In last week's episode, I detailed all of the boundaries that I'm setting with AI, and one of the first things that I mentioned is that I will not give AI access to my banking statements. It is situations like this that make me feel very confident in my decision.

to do so because we never know where that data is going, what it's being used for, and who saw it that shouldn't even have had access to it in the first place.

so what is being done about it? The surveillance pricing story has moved from an FTC study to states deciding that they did not want to wait around and see how bad it could get.

New York decided that if companies are going to be using your personal data to influence a price, you should at least know about it.

New York's Algorithmic Pricing Disclosure Act took effect in November of 2025. The law requires covered businesses using personal data and algorithm pricing to put a disclosure near the price that literally says this price was set by an algorithm using your personal data. of course that's probably going to be in the fine print or something, but at least it's something for us to look for.

In January of this year, California Attorney General Rob Bonta launched an investigative sweep of prominent businesses in retail, grocery, and hotel sectors. His office is asking how companies use browsing history, shopping history, location, demographics, inferred information, and other personal data to set prices. California is also determining whether unexpected use of personal data for individualized pricing can violate the California Consumer Privacy Act.

One interesting thing to note here is I think we should pay very close attention to the language that they're using around this. We're seeing companies and regulators use terms like algorithmic pricing, individualized pricing, and personalized pricing. None of these automatically mean surveillance pricing, but if I see one of those phrases, my next question is going to be are they using personal data to influence what this person pays or not? Because I don't want these practices to be hiding under some other terms. In Maryland, Governor Wes Moore

Has just signed the Protection from Predatory Pricing Act in April, making Maryland the first state to enact a law aimed specifically at personalized grocery pricing. This will take effect on October 1st. They did get some critique from consumer reports saying that there are exemptions and weak enforcement, but we don't really know how that will play out, and so we don't know if it'll fully solve the problem.

In New Jersey, just last month they signed the Fair Price Protection Act, which prohibits grocery retailers from using information such as your online activity, location, purchasing history, and other personal data to charge you a different price for an identical product based on what an algorithm thinks you are able or willing to pay. New Jersey also put a one-year moratorium on new electronic shelf labels while the state studies this technology. Thankfully, Congress is also looking at this problem nationally. In March, the House Oversight Committee asked booking.

Expedia, Uber, Lyft, and Instacart to explain their pricing practices and specifically raise concerns about systems that can infer purchase intent, emotional state, willingness to pay, or consumers' pain point.

So this is all still kind of a problem, but I do think it's really cool to see some regulatory action taking place so soon after these reports came out. I feel like, at least in the States, maybe we need to look at this globally, but I do like seeing our representatives actually take action to protect consumers and hold these companies accountable. I feel like a lot of times when algorithms are doing something unfavorable, they are sometimes more advanced and hard to explain and so complex that they find it hard to really take regulatory action.

action and so I'm happy to see some sort of systematic change happening here.

I also just want to be very clear that there's so much about this situation that we don't know.

We know the technology exists. We know that different people have received different prices for identical products. We do not have a public list of major retailers participating in surveillance pricing, and we also don't know how widespread this is.

I think it is reasonable to assume that a decent number of us have been impacted by surveillance pricing at this point. They've named so many industries, products, and services where they're not only common but essential. But what can we do about it? So the frustrating answer is that there's no single action you can take that guarantees you will never encounter surveillance pricing, at least not right now. avoiding a specific list of supposedly

Suspected companies is probably impossible anyway. A relatively small number of platforms, retail groups, and tech vendors can serve hundreds of brands and millions of customers. But you know what I'm gonna say? Work on that data hygiene. You should absolutely be thinking about how to reduce the amount of unnecessary data available to these brands in the first place.

Here are four ways that you can make yourself a little harder to profile.

The first one is dial back that location access and do it across all of your devices. The FTC specifically named location as one of the data types relevant to surveillance pricing systems. Go through your phone, look at which shopping, restaurant, travel, delivery, retail apps, see which ones have your location. And I would be especially skeptical of the precise location access or the always-on location for an app that does not actually need those permissions to function.

Anytime my iPhone asks whether I want to share my location, I usually choose don't allow. Sometimes I'll choose allow while using app if the location is actually necessary for the app to work. Like Uber Eats is a great example. I'll let it use my location while I'm actively using the app because it needs to know where I am so I can deliver the food. But there's just no reason for it to have access to my location all day in the background. And most apps really don't need that anyway. On desktop, review location permissions in your browser.

Chrome, Safari, Firefox, and Edge all let you see which websites have permission to access your location, and you can revoke any of them. Second one, reduce cross-site and cross-app tracking. Use the privacy controls available on your phone and browser to limit tracking across companies. Turn off allow apps to request to track, or just review those permissions app by app.

Whenever an app asks if they can track across apps, I always say no.

Also, think about using a privacy-focused browser like Brave or DuckDuckGo. They have stronger built-in tracking protections than a standard browser. If your browser supports global privacy control, that is also worth enabling. In states where the signal is legally recognized, it can automatically communicate that you do not want your personal information sold or shared.

Yeah.

The third one is use private browsing and a VPN. Incognito or private browsing can help remove some signals tied to cookies and existing logged in browser sessions, but it won't remove all of them. It's worth investing in a VPN. A VPN is going to conceal your IP address and make it harder to use that signal to infer your location.

Neither of these are anonymous and neither will guarantee you a different or cheaper price. But I do think they're both useful for limiting data sharing overall and very useful for comparison shopping. Which brings me to my last tip, which is just to simply compare the price that you see.

Try checking another retailer or another booking platform. Go directly to the company website if you're not already there. Maybe try going to the same website while logged out.

I do this all the time with Rideshare. Every single time that I order a ride, I check Uber, I check Lyft, and I check my taxi app because I know at any given moment one could be way cheaper than the other. And it is not a small difference. And also, it's not that one app is always cheaper than the other. It's always kind of like varying between the two. It's very interesting.

There's a really cool tool that I found recently for Amazon products called Camel Camel Camel. I'll add the link in the description. But they show the historical price of an item, which is useful for figuring out whether a supposed deal is actually a deal.

Overall, you can't browser setting your way out of surveillance pricing right now because we just don't have that much transparency into where it actually is. But I think limiting your data footprint overall can really help you avoid that extra tax that might be coming your way.

All in all, I think surveillance pricing is super icky. We, as consumers, should be allowed to make good financial decisions for ourselves. And I think that anything that uses my personal profile to interfere with that choice feels like a bit of a bastardization of capitalism to me. Part of being a consumer in a market is being able to compare prices, optimize your spending, find a deal, and decide for yourself what something is worth to you.

this whole situation is also like such a bait and switch because for years companies have justified collecting enormous amounts of information because they said it would make ads more relevant and products more personalized. But then turning around and using that information to find the absolute highest price that we're willing to pay for a product and taking away any chance that we have at cost savings is gross. I've never felt

like targeted advertising was a benefit to the consumer, but we have more obvious proof now that it's truly just a benefit to the seller.

I also think there's something ominous about a company noting your as they called it emotional state or your level of desperation to change a price. Weird. I think that's weird.

At the end of the day, they can make all the justifications they want, but my thing is if it's ethical and if it's totally okay, why don't we know about it? Why did the FTC have to launch a formal investigation into it? And why are they being so sneaky? I don't know.

I think everyone deserves to know about this. I hope that everyone does learn about this. Tell your friends about this. Honestly, I think this should be national news. Okay, I want to share two quick news bits.

First is that Comcast is turning Wi-Fi routers into motion sensors. Comcast just rolled out a feature called Wi-Fi motion to millions of newer Xfinity routers. It uses disturbances in your

existing Wi-Fi signal to detect movement inside your home, which can send you alerts through the Xfinity app when it senses activity. The features work on XB7 gateways and newer models. It's also opt-in.

I know what you're thinking. Siara that sounds super boring. I know. But I want to remind you of my conversation with Aza Raskin. He warned us about the technological surveillance as it pertains to Wi-Fi signals and router networks. I'm gonna run the clip real quick.

So I don't know, this one did make me think. My biggest thing is like, who even asked for this feature? Also, the privacy policy is kind of shady. Comcast says information generated by Wi-Fi motion may be disclosed to third parties without further notice to you in connection with law enforcement investigations, disputes involving Comcast, subpoenas, or court orders.

I guess we can appreciate that this feature is opt-in.

So if you think motion sensing through your router is useful, you can absolutely make that choice. I personally do not need my internet router generating a record of movement inside of my home. Especially when they could disclose that data in certain legal and law enforcement circumstances without notifying me. Like nothing crazy is happening in my apartment, but it's giving flock is in my kitchen. So that is a super hard pass for me. Second news story is good news for consumers.

In New York. Starting October 1st, New York City is implementing a new click-to-cancel rule for subscriptions. If a company lets you sign up for a subscription through one method, it has to give you a straightforward way to cancel through that same method.

To me, this is all about user experience design. I think sometimes companies use UX design to siphon more money from you and get you to do more things and grab more data that you didn't intend to give them. So I really like that this is happening and I hope that it spreads to more places. I have been burned. I've been burned up multiple times. I think I'm still being burned by Adobe. So to me, this is great. I hope it becomes a more nationwide expectation of brands because there are definitely companies that are just taking advantage.

Businesses that violate the rule can face civil penalties starting at \$525 per violation, and consumers may also be entitled to refunds. New York City estimates that the rule could save residents as much as \$162.5 million a year. Nice. That is everything that I have for you this week.

I'm feeling pretty grateful to the FTC and to Consumer Reports for filling us all in on the information. Even though we don't have specific names, we do have some suspects. So that's something. I think surveillance pricing is really one of those issues that should change the way that we look at the data economy. The more companies know about us, the more opportunities they have to shape our choices and now potentially our expenses. This is why I am always

talking about how data is valuable and data is currency. There is a reason that data has been called the new oil for years.

So when you give data to a company, you should consider it a transaction because it is costing you something. Data privacy is not some abstract principle anymore. Alright, I'm getting off my soapbox.

On that note, save your coins, protect your data, and have a wonderful weekend. I hope you get a chance to log out soon. Bye.