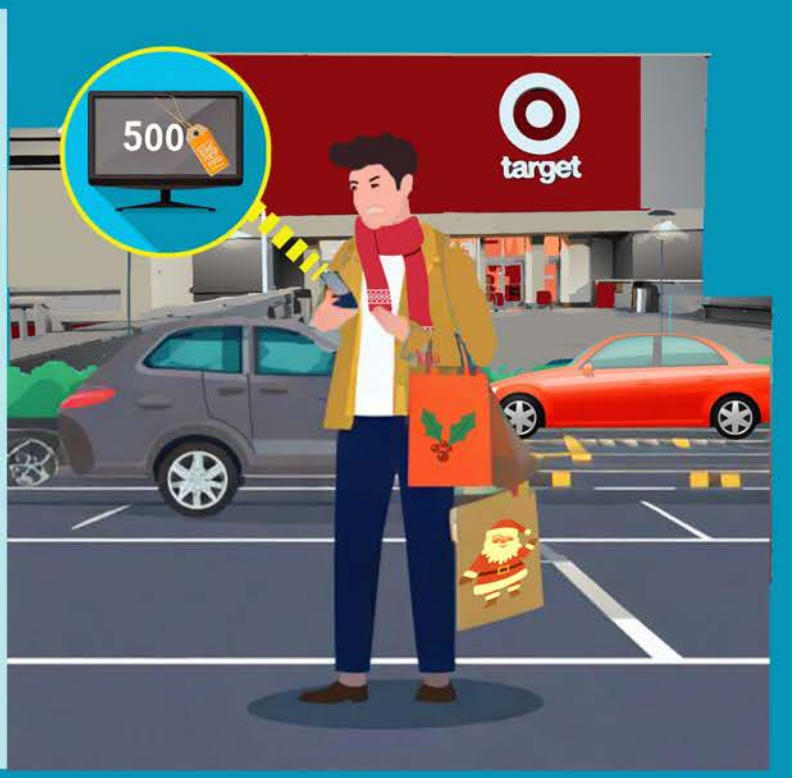
DECEMBER 2024

SURVEILLANCE PRICE GOUGING

BY JUSTIN KLOCZKO



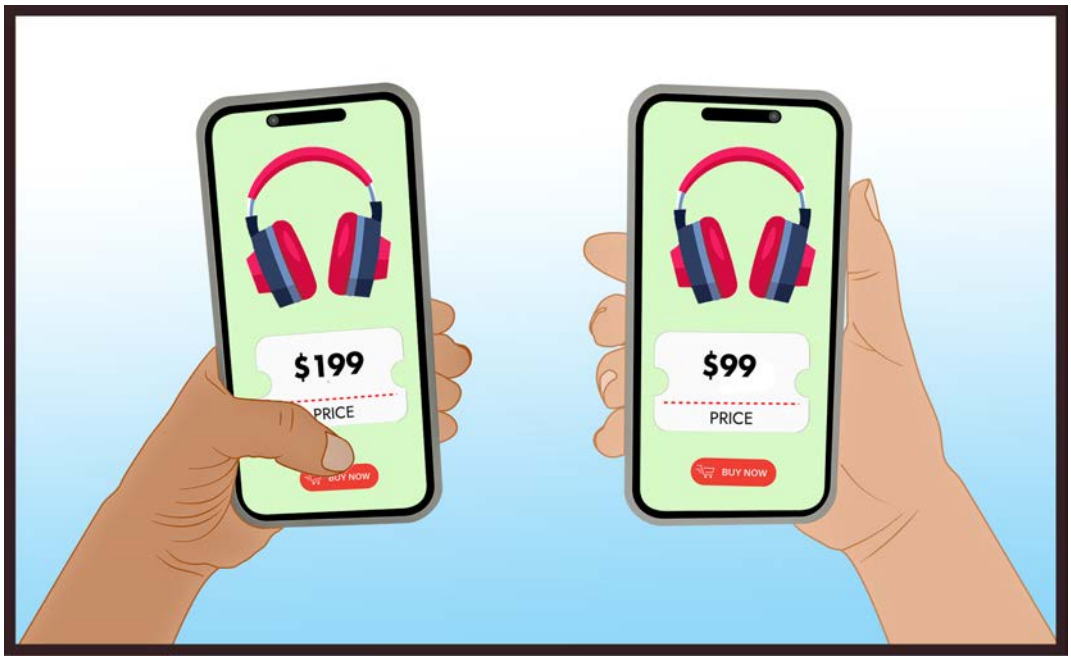
PEOPLE ARE CHARGED ***DIFFERENT*** PRICES FOR THE ***SAME*** PRODUCT BASED ON SURVEILLANCE

Consumer Watchdog

Surveillance Price Gouging

People are charged different prices for the same product based on corporate surveillance of their lives. Here's how to stop that.

By Justin Kloczko



Introduction

What if you're being charged more for the same product than another person based on surveillance of your behavior by the companies you do business with?

Consumers are increasingly charged different prices based on their data and on AI-driven surveillance that makes assumptions about their eagerness to pay. This creates a scenario where a different price is sometimes being offered for the exact same product depending on the buyer's circumstances.

Target charged people $100 more for a t.v. when they were in a Target parking lot versus when they were in another location. Orbitz learned that Mac users spend more money to stay at hotels and charged them more than non-Mac users. Over at Amazon, prices change over 2.5 million times a day, meaning the average cost of a product changes about every 10 minutes.

It's price gouging based on predictive behavior.

A lot is not known because of corporate secrecy, but what we do know now is companies are experimenting with surveillance pricing as a way for businesses to weaponize personal data against you in order to charge more. A Yale study found personalized pricing increased profits for airlines by 4-5%.

Uber reportedly charged different prices based on whether the customer used a corporate credit card. Farmers Insurance overcharged its longtime California customers 4%-13% more in premiums each year, just because the company judged them unlikely to shop around, according to a recently settled case.

It's price gouging based on predictive behavior.

Without more transparency, we don't know how far surveillance pricing goes.

Today, the wealthier a person is, the less they're likely to pay, and vice versa. A lower credit score means higher prices offered to consumers of many products. For example, a study of broadband internet offers to 1.1 million residential addresses showed the worst deals given to the poorest people.

"Areas that tended to see the discounted prices had a higher average income than areas that tended to see higher prices," reported the *Wall Street Journal*.

Dynamic pricing is when the price of a product fluctuates, often by the minute, based on real time supply and demand derived from algorithms and real time data analysis. While dynamic pricing is based on market forces like supply and demand, as well as

competition, surveillance pricing is not. Surveillance pricing is based on you. It is based on personal data that is increasingly detailed and analyzed by AI. *The American Prospect* called it "One Person, One Price."

Consumers have been ripped off for as long as there was an item to sling, but what makes things different today is how easy it is to buy something online with a tap of your phone. How would you know if you are being surveillance priced?

This report serves as a primer for an emerging phenomenon, as well as a road map on how to address it.

Surveillance Pricing and E-Commerce

Nearly 10 years ago, the recruiting company ZipRecruiter, who charges companies to find employees, tested out surveillance pricing by asking companies about their location, industry and employer benefits. And what ZipRecruiter found was when they incorporated the data about location and benefits into its pricing, profits increased 84 percent.

Initially, ZipRecruiter charged employers $99 a month.

"The results indicated that ZipRecruiter could increase profits by moving to a higher price, and the researchers calculated that the optimal price was between $249 and $399," wrote *The Chicago Booth Review.*

That was the beginning of surveillance pricing. Now it's likely everywhere, and it's invisible. A major part of why it's hard to see is because it occurs in the silos of people's devices without other people knowing about it. If two people are shopping for rental cars on their respective devices, there is an element of isolation that keeps the price fixing concealed. It's not like we're walking into Nordstrom and being shown different prices that everyone can see. If that was the case, there would be riots on the streets.

Surveillance pricing can occur while shopping for groceries, electronics, hotels, and flights. It is an emerging phenomenon that is hard to prove, but the following are known and suspected cases:

Target: Target charged people more when they were in a Target parking lot versus when they were in another location, according to NBC affiliate KARE11. Target determined people who are already in their parking lot were willing to pay more. For example, a t.v.

on the Target app was priced at $499.99, but once the person entered the company's parking lot the price went up $100, to $599.99.

The Princeton Review: The test prep company charged customers shopping online from zip codes that contained a higher number of Asians more money, according to *ProPublica.*

Staples: Staples.com charged people more for the same stapler if they knew a person had fewer options, such as being near a competitor, according to the *Wall Street Journal*.

Orbitz: Orbitz learned that Mac users spend more money to stay at hotels and charged them more than non-Mac users, according to the *Wall Street Journal*.

Amazon: The enormous amount of data at Amazon's disposal allows it to change prices over 2.5 million times a day, meaning the average cost of a product changes about every 10 minutes. Prices are fluctuating all the time based on real-time data. The price a user sees could depend on how often they've visited a product page, among other factors.

Rideshare: Uber charges prices based on destinations, so two customers leaving the same place at the same time and going the same distance—but to different destinations—pay different prices. That's dynamic pricing, but it's unclear if the company is using surveillance pricing.

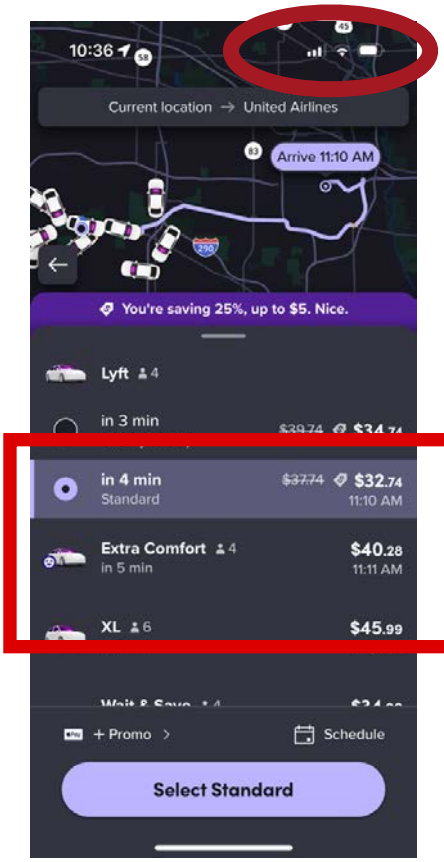
People have reported being charged different Uber fares when using a corporate credit card over a personal credit card. In 2016, a data scientist at Uber said the company knew that people were more willing to pay a higher fare when their phone batteries were low. So does Uber charge people with low batteries more than people who don't? While the company said, "We absolutely don't use that" information, one must wonder why Uber hired a data scientist in the first place, if it wasn't intending to manipulate prices based on people's behavior?

Uber and Lyft made statements that put into question whether it does indeed use surveillance pricing. For one, it has admitted to calculating fares based on "trip purposes."

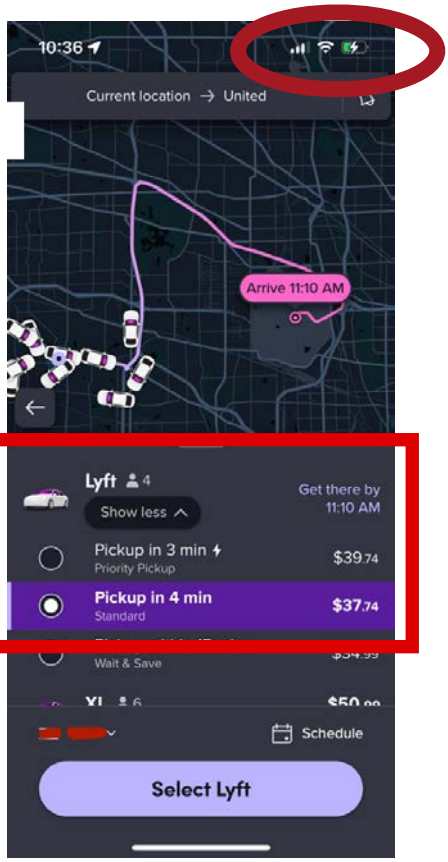
Uber said that "land-use/neighborhood patterns, trip purposes, time of day, and other effects" go into pricing. Lyft said, "There are many factors that go into pricing — time of day, trip purposes, and more."

"Trip purposes" can certainly mean a lunch date, appointment, or other nonmarket factors.

To test it out, Consumer Watchdog requested rides from rideshare companies. Both rides were requested from the same company at the same time, the routes had the same origin and destination, and both were identical in distance and route traveled. However, one person paid $5 more on Lyft than the other person using Lyft, and one person paid $1 more on Uber than the other person using Uber. It's unclear why:



Lyft fare quoted with more battery power.



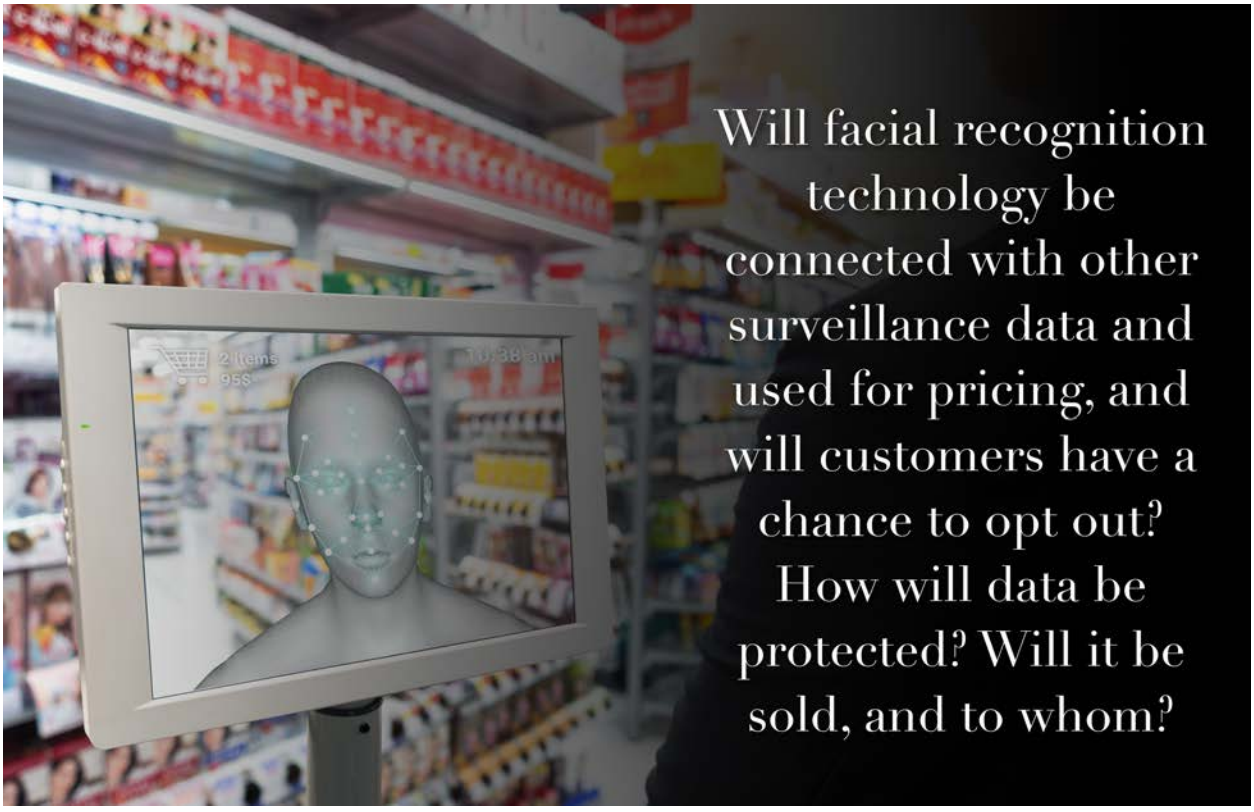
Lyft fare quoted with less battery power.

Insurance: The car insurance industry has used our personal driving data, known as telematics, to determine premiums in states where they are allowed to do it. It is the ultimate surveillance pricing. A black box in your car or an app on your mobile phone lets the companies collect everything from brake patterns, speed, and cornering to what time of day and where people drive, according to a report by Consumer Watchdog. It is illegal for companies to refuse to sell insurance to a driver based on income or race. However, many insurance companies' driving scores get at that information in other ways. Time of day is used by nearly all companies, and late night or early morning drivers pay the most.

These drivers are also more likely to be workers on the third shift, and disproportionately low income and people of color. Liberty Mutual, for example, said that it collects data on time, location, braking, phone type, and vehicle diagnostics. While the industry says consumers' driving habits should drive premiums, the fact is that much of the data the companies use to determine premiums is not proven to be related to the risk of loss.

For example, a Consumer Reports investigation found multiple insurance companies—including Travelers, Allstate and Progressive—were miscategorizing drivers' braking speeds as dangerous "hard braking," when Consumer Reports considered the same braking speeds safe, and potentially a sign of an alert driver.

Insurance companies have also figured out how sensitive consumers are to premium increases and have been able to raise rates without losing customers based on surveillance of your habits. This price optimization tactic is calibrated thanks to a trove of data giving companies incisive details regarding brand loyalty and shopping behavior. Companies "optimize" their price based on your perceived sensitivity to higher prices and loyalty to a brand, which has nothing to do with the actual cost of insuring you, your home or your vehicle. Consumer Watchdog intervened in a case against Farmers Insurance and found it overcharged its longtime California customers 4 - 13 percent more in premiums each year than it should have – $26 million to $29 million a year in total.



We also found that Allstate overcharged its best California customers—among its safest drivers and most profitable policyholders—by approximately $1.03 billion from 2012 to 2021.

Such overcharges are barred by Proposition 103, California's voter-approved insurance reform law. But consumers in other industries aren't so lucky….

Future Fears

Surveillance pricing is a novel issue, and it's not known how widespread it is or exactly how it works. The Federal Trade Commission subpoenaed several companies, including JPMorgan Chase, Mastercard and McKinsey, to learn more about it. But at the time of this writing, it is unclear if we'll find out more given the transition under the new incoming new presidential administration.

Other things are happening too. Kroger and Wal-Mart plan on installing digital price tags on shelves by 2026, so between the time you grab a loaf of bread and check out the price may increase.

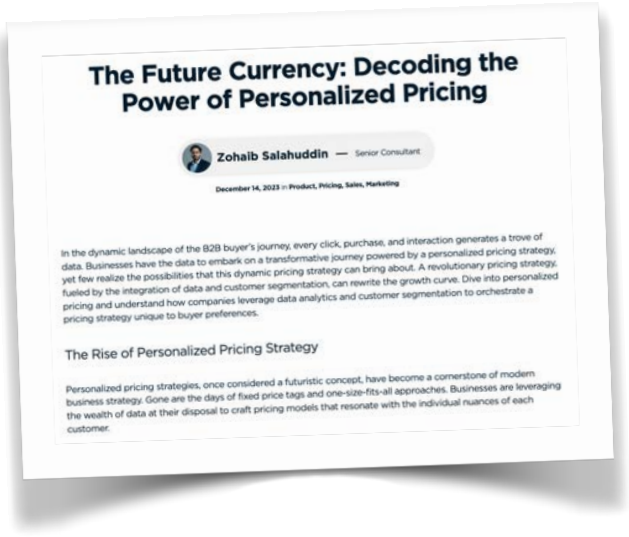
Both companies also plan to incorporate facial recognition technology for targeted coupons. It begs the question: Will facial recognition technology be connected with other surveillance data and used for pricing, and will customers have a chance to opt out? How will data be protected? Will it be sold, and to whom?

Data is the driving force of corporate consolidation such as the Kroger-Albertson's merger. A big part of why companies are seeking to buy other competitors is not just because of their tech or audience, but because of the data they have. That was part of Kroger's argument for why it should be able to acquire Albertson's. It told a federal judge during its antitrust trial with the FTC that the merger is good because data held by

Albertson's helps fuel surveillance advertising, which is a benefit to consumers, and that those profits will be used as cost savings.

The food giant has already been accumulating a mountain of analytical data. Almost 10 years ago it acquired a company called Dunnhumby Data Assets, which says it has access to "some 770 million profiles" and uses "first party retail data from nearly 1 of 2 US households and more than two billion transactions." In addition, Kroger has a marketing arm that synthesizes and sells personal data called "Precision Marketing." These same brands it sells to also stock the shelves of its grocery stores across the country.

Right now, Walmart wants to buy Vizio, in order to flash direct-to-consumer advertising over a smart T.V. Companies believe this to be the future, a complete union of entertainment and commerce. But a letter from 19 groups opposing the merger notes, "Acquiring Vizio will enable Walmart to further grow its business lines that rely on extracting, monetizing, and exploiting consumer data."


The Future Currency: Decoding the Power of Personalized Pricing

Zohaib Salahuddin — Senior Consultant

December 14, 2023 in Product, Pricing, Sales, Marketing

In the dynamic landscape of the B2B buyer's journey, every click, purchase, and interaction generates a trove of data. Businesses have the data to embark on a transformative journey powered by a personalized pricing strategy, yet few realize the possibilities that this dynamic pricing strategy can bring about. A revolutionary pricing strategy, fueled by the integration of data and customer segmentation, can rewrite the growth curve. Dive into personalized pricing and understand how companies leverage data analytics and customer segmentation to orchestrate a pricing strategy unique to buyer preferences.

The Rise of Personalized Pricing Strategy

Personalized pricing strategies, once considered a futuristic concept, have become a cornerstone of modern business strategy. Gone are the days of fixed price tags and one-size-fits-all approaches. Businesses are leveraging the wealth of data at their disposal to craft pricing models that resonate with the individual nuances of each customer.

"Personalized pricing strategies, once considered a futuristic concept, have become a cornerstone of modern business strategy," said the Cortado Group.

A good indicator of how big surveillance price gouging is becoming are corporate consultants such as McKinsey and Cortado Group.

"Personalized pricing strategies, once considered a futuristic concept, have become a cornerstone of modern business strategy," said the Cortado Group.

McKinsey's take on surveillance pricing: "Our experience shows that such transformations, when done well, can enhance pricing to generate two to seven percentage points of sustained margin improvement with initial benefits in as little as three to six months."

Loopholes and Protections

Depending on several factors, surveillance pricing could violate deceptive practices and unfair competition laws. Companies often change prices based on location and demand, like Ticketmaster's controversial dynamic pricing algorithm. It ultimately comes down to if a company is misleading, and companies often get away with it by obscuring their data collection policies through convoluted notice and consent forms.

Target, for example, was forced to pay $5 million in civil penalties and stop its geofence price switching after it came out that prices for a t.v. went up once consumers entered the store's parking lot. What Target got in trouble for was not charging different prices, per say, but not disclosing that there was a lower price. The judgment also stopped Target from changing prices on its app based on the user's geographic location.

On the data privacy side, there is no federal data privacy law. And in California, the California Consumer Privacy Act (CCPA), while giving people more control over their data, appears to have a loophole that allows companies to charge different prices based on their data. The law's intent was to provide people a discount or incentive for providing data to a business, but it does not bar using data against the person they took it from.

Under *1798.125* of the *CCPA*, Consumers' Right of No Retaliation Following Opt Out or Exercise of Other Rights, it states:

> *Nothing in this subdivision prohibits a business, pursuant to subdivision (b), from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data.*

It seems like authors did not have surveillance pricing in mind when drafting the CCPA.

Solutions

There is no state or federal law protecting consumers from surveillance price gouging. There needs to be a law addressing it. There needs to be a right to standard pricing and safeguards against surveillance pricing.

Consumer Watchdog recommends the following provisions to be enacted in some form of legislation:

- Businesses must provide a notice to consumers on their websites or during checkout that informs them if personal data, and what kind of data, is being used to generate prices.
- Businesses shall be barred from using personal data, such as geolocation, purchasing history and IP address, when setting or adjusting prices without first notifying consumers.
- Consumers shall have the right to "Standard Pricing," defined as the price that would have been offered if no personal data was used in generating the price.
- Attach a financial penalty to businesses that violate the law.

The first step is increased awareness. About 25 years ago, Amazon tried surveillance pricing for DVDs, but people figured it out after someone deleted their cookies and received a lower price. A public outcry ensued, Jeff Bezos issued an apology, and refunds were sent out. Today that's not happening. More people need to know about behavioral price gouging, so adequate protections can be put in place.