Ever wonder why your price is different from your friend's for the same product? It’s not a coincidence—companies are using your personal data to set your price.

Have you ever noticed a product’s price changing right before your eyes—or wondered why a friend pays less for the same service? It’s not your imagination. Companies are using every bit of personal information they can get—from your location to your browsing history—to decide how much they’ll charge you.

What is Surveillance Pricing?

Surveillance pricing involves businesses collecting detailed data about consumers (like your demographics, web habits, and even mouse movements) to set individualized prices. The Federal Trade Commission (FTC) recently released a report on eight companies that use these “shadowy” surveillance pricing methods. They found these third-party providers routinely gather data and use AI-driven algorithms to charge people different amounts for the exact same products or services.

Price is Increasingly Dynamic

Aspect	Details
Definition	Surveillance pricing determines the price of a product based on consumer data, location, and timing.
Price Complexity	Pricing changes can occur at different frequencies (minutes to monthly).
Personalization	Different people may see different prices based on their location, channel, or data profile.
Scale and Efficiency	Companies can use tools to scale pricing complexity while optimizing resources.

Why It Is Important

1. **Privacy Concerns**
    - Your personal data—like location info or even your health status—can be used in ways you never intended. In some extreme cases, data brokers have created lists of individuals with certain diseases to target them with questionable treatments.
2. **Unfair Competition**
    - If people are constantly shown different prices, it gets harder to compare and shop around fairly. That can lead to distorted markets and even higher prices overall.
3. **Consumer Protection**
    - As these strategies become more prevalent, consumers risk being exploited without ever knowing they're paying extra based on invisible data profiles.

Inside the Pricing Machine

- **Data Sources**: Everything from your IP address and social media activities to the items in your abandoned online shopping cart can be used to decide how much you'll pay.
- **Regulatory Spotlight**: FTC Chair Lina M. Khan says it's vital to shine a light on how these "pricing middlemen" operate—especially when they collect information from multiple sources to create incredibly detailed consumer profiles.
- **Insurance-Style Risk Assessment**: Surveillance pricing is nothing new in the insurance industry, where health, lifestyle, and location data can mean higher rates or even denial of coverage. Now, other industries are catching up with similar tactics.

Take Control: Here's How to Protect Yourself

It's easy to feel overwhelmed by the idea of companies tracking and monetizing your every move online. But there are steps you can take right now to protect yourself:

1. **Think Twice About What You Share**
    - Limit personal details on social media and use only the information that's absolutely necessary when signing up for services.
2. **Review App Permissions**
    - If an app doesn't truly need your location, don't give it access. If you must, select "Allow only while using the app."
3. **Read Privacy Policies**
    - Yes, they can be dull—but they'll tell you how your data might be used.

4. **Block Web Tracking**
    - Use browser based security tools to opt out of tracking cookies, which can help prevent invasive data collection.

By staying informed and taking these small steps, you can reduce the amount of data you share—and help ensure you're not paying more just because your digital footprint says so.