

Insights

WILL THIS BE ON THE EXAM? FTC STAFF ISSUES TWO INITIAL REPORTS ON SURVEILLANCE PRICING

Jan 27, 2025

On January 17, 2025, the staff at the Federal Trade Commission (FTC) released their first results from the FTC's Surveillance Pricing market study. The FTC staff reports, including both a "staff perspective" and an "issue spotlight," give a window into the FTC staff's preliminary concerns about surveillance pricing practices. Notably, both reports are very academic, with the staff perspective discussing solely hypothetical use cases and the issue spotlight serving as a roundup of past articles. These staff reports, however, will not be the last words: FTC Chair Andrew Ferguson has promised a final, complete report on surveillance pricing (or, as he calls it, personalized pricing) in the future. Clients—especially in the technology, financial services, and retail sectors—should pay careful attention to their pricing practices to avoid further FTC or other enforcer scrutiny.

BACKGROUND

Surveillance pricing goes something like this: two individuals shopping online may have vastly different experiences and see varying prices for the same product on a seller's website. A variety of factors influence these price differences, such as the buyer's demographics, location, and past interactions with the seller. Companies collect this data through extensive large-scale data collection practices, both on individual websites or apps and across the internet. Essentially, surveillance pricing leverages consumer information to create customized pricing for each individual or group.

In July 2024, the FTC unanimously issued eight subpoenas using its unique 6(b) authority. ("6(b)" refers to the section of the FTC Act that authorizes such subpoenas, 15 U.S.C. § 46(b).) The FTC subpoenaed eight companies in the financial services, consulting, and analytics sectors to better understand how these companies and intermediaries set individualized prices. The FTC turned its attention to surveillance pricing due to the development of infrastructure that can support its widespread implementation. In recent years, dynamic pricing strategies, such as those used by e-commerce platforms, have flourished. These strategies have not only facilitated extensive data collection but have also created the framework necessary to seamlessly incorporate surveillance pricing into existing business operations.

FTC STAFF'S TWO INITIAL REPORTS

Days before the administration changed, FTC staff issued two reports, a staff perspective based on documents from six of the eight subpoenaed companies and an issue spotlight. Before turning to the substance, it is important to note that both documents are significant departures from the FTC's past 6(b) practice in at least three ways. First, the staff perspective, rather than being a comprehensive evaluation of all of the information submitted by the subpoena recipients, is instead expressly framed as a "pre-publication" or "beta version" of a report. Second, while the staff perspective does cite certain internal documents (all of which are redacted), the various examples of surveillance pricing use cases are all hypotheticals. Third, the issue spotlight—only the second ever issued in the FTC's history—is confusingly "not part of the 6(b) study" nor "based on any non-public information," but rather is a collection of academic articles FTC staff appears to have found useful and issued simultaneous with the staff perspective.

Nonetheless, having agency staff's proverbial "syllabus" will help clients understand what will be asked on the "test," i.e., a potential future enforcement action. Both staff documents indicate that the greatest risks of surveillance pricing to consumers arise in the context of deceptive or unfair practices. FTC staff specifically point to the widespread use of personalized discount codes and coupons, noting that claiming to offer "sales" or "discounts" via surveillance pricing can be deceptive. Since each consumer might pay a different amount based on their specific discount, no single buyer would actually pay the "nominal price" from which the discount is taken.

For example, FTC staff highlight hypothetical concerns about claims like "up to 25% off," arguing that while the discount may apply consistently across buyers, there may not be a true nominal from which the discount is offered. This broad interpretation introduces questions about whether common retail terms like "sale" or "discount" could be deemed deceptive under the FTC's understanding of surveillance pricing.

This interpretation also raises questions about future interpretation and enforcement of state laws like California Business & Professions Code Section 17501. That code requires that, to advertise a price as a "sale" price in comparison with a previous price, the alleged former price must have been the "prevailing market price" for three months preceding the ad. Determining the prevailing market price for the prior months is already a complicated and nuanced undertaking, without taking into account individualized pricing.

Deceptive or unfair practices may also stem from the use of inferred data. In its staff perspective, FTC staff note that the data inputs used to run surveillance pricing tools can vary depending on the tool's intended purpose. A key concern is inferred data—information derived from a consumer's online behavior. For example, actions like adding an item to a cart without completing the purchase or sorting a results list by lowest to highest price can be used to infer details about a consumer's purchase intent or financial situation. The methods used to generate these inferences are diverse and often opaque, making it unclear how certain conclusions are drawn. This is particularly

troubling because systems that support surveillance pricing can continuously collect and analyze data. FTC staff is concerned that shoppers are frequently unaware that their inferred data is being continuously collected, and shoppers may not have explicitly consented to its use. These concerns raise questions about the risks that online businesses may face when utilizing such data in ways that consumers may not fully understand or consent to.

Turning to competition, the two staff reports both raise antitrust concerns and provide important evidence of pro-competitive defenses. In its issue spotlight, FTC staff explain that algorithms used for surveillance pricing can result in pricing that is actually or effectively collusive. This occurs because sellers' algorithms may align their pricing strategies as if the firms had directly colluded. Additionally, multiple sellers might rely on shared data or algorithms, and if sellers agree to use the same algorithm for pricing decisions or share sensitive consumer information with the same third-party provider, this could amount to an anticompetitive agreement. These scenarios raise important concerns about what measures businesses should take to avoid knowingly using the same surveillance pricing data as competitors, which could lead to allegations of price fixing.

On the other hand, the staff perspective suggests that surveillance pricing could promote consumer welfare. The study indicates that these tools have the potential to increase revenues by 2-5% and margins by 1-4%. The staff perspective also acknowledges that surveillance pricing allows companies to reduce costs by enabling businesses to operate more efficiently. And the issue spotlight recognizes that surveillance pricing is just one method of knowing more about a buyer, which has long been a key avenue in competing and maximizing profits. This is important evidence of pro-competitive uses of surveillance pricing.

MORE ANALYSIS NEEDED

These initial findings and insights are not a comprehensive summary of surveillance pricing or all the documents that the FTC has received. Indeed, the FTC has said nothing about any materials received from two of the eight subpoenaed companies, including several large financial services companies. Rather, these staff documents showcase the FTC's preliminary observations, encourage early engagement within the research community, and promote public transparency, particularly in this fast-evolving area of technology. In his dissenting statement, now-Chair of the FTC Andrew Ferguson, joined by Commissioner Holyoak, criticized these preliminary studies as "[s]lowly dripping out information obtained during the Section 6(b) process," which "does not serve the public interest." However, Chair Ferguson agreed with FTC staff that "there is much more work to do," and indicated that a "final, fact-based report" on this topic would be published in the future.

RELATED PRACTICE AREAS

- Antitrust
- International Trade
- Public Policy & Government Affairs
- Retail & Consumer Products
- Financial Services
- Financial Regulation Compliance & Investigations
- Financial Institutions
- Data Privacy & Security
- Data Privacy, Telecommunications & Collections

MEET THE TEAM



David B. Schwartz

Washington

david.schwartz@bclplaw.com

+1 202 508 6086



Merrit M. Jones

San Francisco

merrit.jones@bclplaw.com

+1 415 675 3435



Goli Mahdavi

San Francisco

goli.mahdavi@bclplaw.com

+1 415 675 3448



Allison Kim

Atlanta

allison.kim@bclplaw.com

+1 404 572 6747

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be “Attorney Advertising” under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP’s principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.