Issue Spotlight:
The Rise of Surveillance Pricing

1 Introduction

Scope. This document provides an overview of publicly available information from both industry and academia, focusing on the documented growth of surveillance pricing, as well as its scope and impacts on consumers. It provides a detailed overview of surveillance pricing today, discussing some developments and concerns raised in the media, research literature, and other public sources. FTC Staff[1] also highlight areas where, based on our overview, more research is needed.

In July 2024, the Federal Trade Commission voted to use its 6(b) authority to conduct a study into the surveillance pricing ecosystem, focusing on intermediary firms that advertise their use of AI and other technologies along with historical and real-time consumer information to target prices for customers. While exploring similar topics to the 6(b) study, this document is not part of the 6(b) study, nor is it based on any non-public information obtained through that process.

Outline. The document below first provides context and background on surveillance pricing, exploring both how the surveillance pricing ecosystem developed and its scale and scope today. It then gives an overview of some of the concerns raised in the academic literature and public reporting on the surveillance pricing ecosystem, covering its inputs, outputs, and impacts on—and potential harms to—consumers and the marketplace. The document concludes by highlighting areas where, based on Staff's overview, further research is needed.

2 Background

Before the modern era, the prices of consumer goods were often determined through negotiation (or "haggling") between buyers and sellers. Starting in the 1870s, sellers started affixing price tags to consumer goods, streamlining the shopping experience and obviating the need for negotiation.[2] As a result, in the U.S. today, most consumer goods and services are sold on a posted-price basis, meaning the seller presents the buyer with the prices of different goods or services, and the buyer can choose which offers to accept, if any. In general, this model can cover everything from consumer electronics to groceries, whether sold via an e-commerce website or in a brick-and-mortar store.

While the set of products and services offered by a particular seller—and their corresponding prices—were historically the same for most potential buyers under the posted-prices paradigm, that is no longer necessarily the case. Today, particularly online, potential buyers can have different experiences when visiting a seller's business: the offers the seller presents to a particular buyer can depend on a host of other factors, including

[1] The views expressed in this article are those of FTC staff and do not necessarily reflect those of the Commission or any individual Commissioner. Thank you to Staff who contributed: Dr. Alan Mislove, Stephanie T. Nguyen, Marc S. Lanoue, Wells Harrell, Mark Suter, Laura Alexander, Samuel Levine, Kelly Signs, Synda Mark, Dan Salsburg, Ben Wiseman.

[2] Brian Wallheimer, *Are You Ready For Personalized Pricing?*, Chicago Booth Review (Feb. 26, 2018), https://www.chicagobooth.edu/review/are-you-ready-personalized-pricing.

the demographics of the prospective buyer, the buyer's location, the buyer's previous history with the seller or the seller's partners, etc.[3]

This new personalized buying experience is the result of *surveillance pricing*, an ecosystem designed to use large-scale data collection to help sellers maximize their revenues by customizing the pricing, as well as the selection of products and services, offered to each consumer. The descriptions of surveillance pricing differ depending on the source. This document does not attempt to define the term formally or concretely, but rather, surveys and highlights how this term has been described publicly and provides an overview of the related academic literature and public reporting. The FTC's press release for the agency's Surveillance Pricing 6(b) study explains that the 6(b) orders are aimed at helping the FTC better understand the opaque market for products by third-party intermediaries that claim to use "advanced algorithms, artificial intelligence and other technologies, along with personal information about consumers—such as their location, demographics, credit history, and browsing or shopping history—to categorize individuals and set a targeted price for a product or service."[4] One journalist has described surveillance pricing as "a new trend where corporations exploit personal information to set individualized prices for each person."[5]

Importantly, surveillance pricing can incorporate or overlap with features of other well-established mechanisms, such as data scraping, industrial scale data collection, social graphing, personalized pricing, and dynamic pricing. However, surveillance pricing is broader as it encompasses the use of these mechanisms, and others, to collect data on potential buyers and target them with individualized prices for products and services. Additionally, consumer surveillance can have impacts well beyond mere price differences (*e.g.*, to the sets of products offered, to consumers' privacy, to competition, etc.). For example, such impacts can occur when data from consumers' location history, web browsing, and mobile app usage is used by advertising and marketing companies to make inferences about them, which can then affect not only the prices they see when shopping online, but what products and services are made available to them.

Over the past years, the infrastructure necessary to implement surveillance pricing has become more widely deployed. For example, to implement surveillance pricing, sellers will likely need the ability to implement highly dynamic pricing strategies: today, prices and products offered have been observed to change with increasing frequency[6] across industries ranging from food delivery[7] to rental housing,[8] as sellers react to market conditions and test different pricing strategies.[9] The move towards e-commerce has both further enabled surveillance pricing—as the infrastructure for online commerce enables significant data collection and individualized targeting—and made it potentially more difficult to detect, as potential buyers in e-

[3] David Dayen, *The Emerging Danger of Surveillance Pricing,* Jacobin (July 9, 2024), https://jacobin.com/2024/07/surveillance-personalized-pricing-data-collection.
[4] Press Release, Fed. Trade Comm'n, "FTC Issues Orders to Eight Companies Seeking Information on Surveillance Pricing" (July 23, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/07/ftc-issues-orders-eight-companies-seeking-information-surveillance-pricing.
[5] David Dayen, *The Emerging Danger of Surveillance Pricing,* Jacobin (July 9, 2024), https://jacobin.com/2024/07/surveillance-personalized-pricing-data-collection.
[6] Alberto Cavallo, "More Amazon Effects: Online Competition and Pricing Behaviors" (Nat'l Bureau of Econ. Rsch., Working Paper No. 25138, Oct. 2018), https://www.nber.org/papers/w25138.
[7] Alexander MacKay, et al., "Dynamic Pricing and Demand Volatility: Evidence from Restaurant Food Delivery" (Harvard Business School Working Paper, No. 23-007, Dec. 2023), https://sites.harvard.edu/pricing-lab/2023/10/17/dynamicpricingrestaurant/.
[8] Sophie Calder-Wang & Gi Heung Kim, "Algorithmic Pricing in Multifamily Rentals: Efficiency Gains or Price Coordination?" (Working Paper, Aug. 16, 2024), https://ssrn.com/abstract=4403058.
[9] Zach Y. Brown & Alexander MacKay, *Competition in Pricing Algorithms*, 15(2) American Econ. J.: Microeconomics 109 (2023), https://www.aeaweb.org/articles?id=10.1257/mic.20210158.

commerce systems are not necessarily aware of the products and services offered to other potential buyers, or their prices (as they typically would be in a brick-and-mortar store).[10]

The ecosystem that supports surveillance pricing has been enabled by the convergence of multiple technological shifts:

1. **Data.** Today, a rich ecosystem of data surveillance exists, including from advertising and analytics services, data brokers, credit providers, and others.[11] Sellers can build detailed profiles of potential buyers to help inform how they will interact with that buyer.[12]
2. **Algorithms.** Today, a wide range of algorithmic approaches have been developed to use data to make predictions about consumers' behavior. These have been accelerated by fast-moving technologies like artificial intelligence ("AI"), which can make predictions from varied and unstructured data from a variety of sources.[13]
3. **Infrastructure.** Today, systems exist that can help sellers develop and implement surveillance pricing strategies. Due to their personalized nature, e-commerce systems can more easily support surveillance pricing, and sellers have been observed to offer different prices to different potential buyers.[14] There is also increasingly infrastructure in physical stores to support advanced pricing strategies and enable the rapid testing of strategies,[15] such as electronic kiosks that can implement personalized discounts and pricing.[16]

The result is that many interactions between sellers and potential buyers today are informed by data that the seller previously collected or obtained about the buyer.

3 Foundations for Systems that Impact Surveillance Pricing

Based on some academic literature and public reporting, we provide an overview of foundations for systems that support surveillance pricing. These foundations can be distinguished by:

[10] David Dayen, *One Person One Price*, The American Prospect (June 4, 2024), https://prospect.org/economy/2024-06-04-one-person-one-price/.
[11] Reuben Binns & Elettra Bietti, *Dissolving privacy, one merger at a time: Competition, data and third party tracking*, 36 Comp. L. & Security Rev. 105369 (2020), https://www.sciencedirect.com/science/article/abs/pii/S0267364919303802.
[12] Ian Bogost, *You Should Worry About the Data Retailers Collect About You*, The Atlantic, Sept. 13, 2023, https://www.theatlantic.com/technology/archive/2023/09/retailers-consumer-tracking-data-personalized-ads-influence/675181/.
[13] David Gal & Itamar Simonson, *Predicting consumers' choices in the age of the internet, AI, and almost perfect tracking: Some things change, the key challenges do not*, 4(1) Consumer Psychology Rev. 135 (2021), https://myscp.onlinelibrary.wiley.com/doi/abs/10.1002/arcp.1068.
[14] *See, e.g.,* Diego Aparicio et al., *The pricing strategies of online grocery retailers*, 22(1) Quantitative Marketing and Economics 1, 17 (2024) (observing that online grocers use algorithmic pricing to "'personalize prices' at the delivery zip code level" and that the algorithms "trigger multiple price changes a day"), https://link.springer.com/article/10.1007/s11129-023-09273-w.
[15] Sara Ruberg, *Kroger and Walmart Deny 'Surge Pricing' After Adopting Digital Price Tags*, N.Y. Times, Oct. 23, 2024, https://www.nytimes.com/2024/10/23/business/kroger-walmart-facial-recognition-prices.html.
[16] Dee-Ann Durbin, *Stop & Shop using grocery kiosks to make digital-only deals available to more customers*, Associated Press, Dec. 13, 2024, https://apnews.com/article/stop-shop-grocery-deals-digital-coupons-b4f181f9c5cca6e4c9f2e706726f1371.

1. **Scale.** Data is routinely collected at a volume that is well beyond what was possible previously.[17] Moreover, data collection is not confined to a single technology or industry but is collected by numerous sources across industries.[18]
2. **Resolution.** Data is generated by many interactions between a seller and potential buyer, with numerous online services embedding multiple trackers.[19] Such data can be used both to "segment," or group individuals based on shared interests or traits, and to enable targeting online down to the individual.[20]
3. **Constant Collection.** Data can be collected continually, and potential buyers are often unaware of the data that has been collected and often have not explicitly consented to that data collection.[21]

This section covers how academic researchers and practitioners have approached understanding these foundations, focusing first on the *inputs* (*i.e.*, the data that is collected) before turning to the *outputs* (*i.e.*, where the effect may be observed).

3.1 Surveillance pricing inputs

Sellers across industries have realized that knowing more about buyers—their preferences and how they use different products or services—can provide additional avenues for maximizing profits. Early examples of technologies for gathering such information on consumers include "auditmeters"[22] which recorded the radio stations to which homes were listening. Later examples included more passively collected data, such as the newspapers and magazines to which consumers subscribed,[23] the products that buyers purchased at grocery stores,[24] and the movies that consumers rented from video rental stores.[25] At the same time, credit reporting agencies and other financial firms[26] began to use data they collected to offer data analytics and targeting information to advertisers. Today, sellers and various third parties collect large amounts of data on consumers—including their purchase histories, their physical movements, their communications, their

[17] Cong. Research Serv., *Online Consumer Data Collection and Data Privacy* (No. R47298, Oct. 31, 2022), https://crsreports.congress.gov/product/pdf/R/R47298.
[18] *See* Michael Kwet, *In Stores, Secret Surveillance Tracks Your Every Move*, N.Y. Times, June 14, 2019, https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html; R.J. Cross, *How Mastercard sells its 'gold mine' of transaction data*, U.S. PIRG Education Fund (Sept. 23, 2023), https://pirg.org/edfund/resources/how-mastercard-sells-data/; Kashmir Hill, *Automakers Are Sharing Consumers' Driving Behavior with Insurance Companies*, N.Y. Times, Mar. 11, 2024, https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html.
[19] Steven Englehardt & Arvind Narayanan, *Online Tracking: A 1-million-site Measurement and Analysis*, Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security 138 (Oct. 24, 2016), https://dl.acm.org/doi/10.1145/2976749.2978313.
[20] Salim Chouaki et al., *Exploring the Online Micro-targeting Practices of Small, Medium, and Large Businesses*, 6 Proceedings of the ACM on Human-Computer Interaction 1 (Nov. 2022), https://dl.acm.org/doi/10.1145/3555103.
[21] Stefan Larsson et al., *Notified but Unaware: Third-party Tracking Online*, 8(1) Critical Analysis of Law 101 (2021), https://cal.library.utoronto.ca/index.php/cal/article/view/36282.
[22] Laurence N. Gold, *Technology in television research: The meter*, 6(1) Marketing Research 57 (1994).
[23] Fed. Trade Comm'n, Data Brokers: A Call for Transparency and Accountability (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.
[24] Chiara Mauri, *Card loyalty. A new emerging issue in grocery retailing*, 10(1) J. of Retailing and Consumer Services 13 (2003). https://www.sciencedirect.com/science/article/abs/pii/S096969890200036X
[25] Michale W. Miller, *Coming Soon to Your Local Video Store: Big Brother*, Wall St. J., Dec. 26, 1990, at 9.
[26] Albert B. Crenshaw, *Credit Card Holders to be Warned of Lists*, Wash. Post, May 13, 1990, https://www.washingtonpost.com/archive/business/1992/05/14/credit-card-holders-to-be-warned-of-lists/ecac8f90-4291-4c84-8f0f-c27f374bd64b/.

medical information, and other highly sensitive data—sometimes without consumers' knowledge or consent.[27]

The rapid development of computer and mobile technologies has only increased the scope and granularity of collected data: mobile devices now routinely run applications that embed third-party library code for the purpose of tracking users,[28] websites use a variety of techniques to track browsing across the web,[29] and even vehicles collect data on consumers for resale to third parties.[30] Moreover, the recent progress in fast-moving technologies like AI presents new opportunities for data use by sellers, enabling potentially easier translation of input data into actionable pricing and marketing strategies. In particular, the online advertising ecosystem is a common source for data collection on individuals. Now an industry with over $225 billion in yearly revenue in the U.S. alone,[31] this ecosystem is largely driven by online behavioral advertising,[32] which involves thousands of firms offering services including supply- and demand-side platforms, ad delivery networks, content distribution networks, data management platforms, retargeting, and many more.

The following is an overview of the academic literature and public reporting on the data that can be used to implement surveillance pricing: what data is collected, how is that data collected, and to whom is that data disclosed.

3.1.1 Data collected by sellers directly

Many sellers directly track customer spending patterns as a mechanism to inform pricing strategies; such data has been understood— even before the modern e-commerce era—to provide significant advantages when used to target coupons and discounts. In fact, one study found that knowing information about even a single purchase could improve revenue on coupons by 50 percent relative to sending coupons to everyone.[33] Retailers often track interactions with potential buyers, using strategies such as "ad retargeting" to try and turn such data into additional sales.[34] Brick-and-mortar retailers have also explored technologies that can track consumers as they browse through stores, potentially offering promotions as the data is collected.[35]

---

[27] Justin Sherman, Report: Data brokers and sensitive data on US individuals, Duke University Sanford Cyber Policy Program (2021), https://techpolicy.sanford.duke.edu/report-data-brokers-and-sensitive-data-on-u-s-individuals/.
[28] Abbas Razaghpanah et al., *Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem*, Proceedings of the 2018 Network and Distributed System Security Symposium (Feb. 2018), https://www.ndss-symposium.org/wp-content/uploads/2018/02/ndss2018_05B-3_Razaghpanah_paper.pdf.
[29] Steven Englehardt & Arvind Narayanan, *Online Tracking: A 1-million-site Measurement and Analysis*, Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security 138 (Oct. 24, 2016), https://dl.acm.org/doi/10.1145/2976749.2978313.
[30] Jen Caltrider et al., *It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy,* Mozilla *Privacy Not Included (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/.
[31] Interactive Advertising Bureau, Internet Advertising Revenue Report: Full-year 2023 results (Apr. 2024), https://www.iab.com/wp-content/uploads/2024/04/IAB_PwC_Internet_Ad_Revenue_Report_2024.pdf.
[32] Sophie C. Boerman et al., *Online Behavioral Advertising: A Literature Review and Research Agenda*, 46(3) Journal of Advertising 363 (2017), https://www.tandfonline.com/doi/full/10.1080/00913367.2017.1339368.
[33] Peter E. Rossi et al., *The Value of Purchase History Data in Target Marketing,* 15(4) Marketing Science 321 (1996), https://pubsonline.informs.org/doi/10.1287/mksc.15.4.321.
[34] Navdeep S. Sahni et al., *An Experimental Investigation of the Effects of Retargeted Advertising: The Role of Frequency and Timing*, 56(3) Journal of Marketing Research 401 (2019), https://journals.sagepub.com/doi/10.1177/0022243718813987.
[35] Michael Kwet, *In Stores, Secret Surveillance Tracks Your Every Move*, N.Y. Times, June 14, 2019, https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html.

Retailers are now directly monetizing the data they collect, with some even developing their own advertising networks to fully realize the value of this data.[36] And the collection and sharing of spending patterns are not limited to consumer-facing retailers; reporting indicates that financial firms—who observe a much broader view of consumers' spending patterns in the course of their business—sometimes sell that data as well.[37]

3.1.2 Data from web browsing

Web browsing data represents an attractive source of data for sellers, as knowing which websites a potential buyer has visited can provide insights into the buyer's general preferences, specific products they are considering purchasing, their health status, and many other topics. As a result, one of the most robust and mature ecosystems for data collection is the web's advertising ecosystem, which relies on a robust set of tracking technologies to collect data on users.

Third-party content. Many popular web services and platforms provide elements for other website operators to include on their sites; often, these can be used to track users. Their presence forces a user's web browser to contact a server operated by the platform, which can then log information about the user's browsing patterns. These elements can take different forms, including spots to serve advertisements,[38] invisible 1x1 "tracking pixels,"[39] buttons that allow users to "share and like" content on social networking services, and analytics JavaScript that provides website operators with statistics on who visits their website. Elements from popular web services and platforms are deployed on a large fraction of websites today, meaning a significant amount of users' web browsing is regularly observed by third parties.[40]

Cookies. Web browsing cookies have long offered a mechanism to track users' web browsing by both first parties (*i.e.*, the website the user is visiting) and third parties (*i.e.*, other websites the first-party website includes content from).[41] While the single-origin policy implemented by web browsers attempts to limit the ability for different third-party domains to link a single user visit, it can be circumvented by third-party websites that exchange data through techniques like cookie synchronization.[42] Recently, there has been a movement away from supporting third-party cookies (some web browsers now block them by default[43]), though many popular web browsers still support them.

Browser fingerprinting. With techniques like cookies and third-party content being increasingly subject to privacy controls, web platforms and services have developed alternate approaches to uniquely identify users

---

[36] David Doty, *Walmart, Target, And Other Mega Retailers Leverage First-Party Data To Become New Media Giants*, Forbes, Apr. 26, 2022, https://www.forbes.com/sites/daviddoty/2022/04/26/walmart-target-and-other-mega-retailers-leverage-first-party-data-to-become-new-media-giants/.
[37] R.J. Cross, *How Mastercard sells its 'gold mine' of transaction data*, U.S. PIRG Education Fund (Sept. 23, 2023), https://pirg.org/edfund/resources/how-mastercard-sells-data/.
[38] Juan Miguel Carrascosaa et al., *I always feel like somebody's watching me: measuring online behavioural advertising*, Proceedings of the 11th ACM Conference on Emerging Networking Experiments and Technologies (Dec. 2015), https://dl.acm.org/doi/10.1145/2716281.2836098.
[39] Paschalis Bekos et al., *The Hitchhiker's Guide to Facebook Web Tracking with Invisible Pixels and Click IDs*, Proceedings of the ACM Web Conference 2023 (Apr. 2023), https://dl.acm.org/doi/10.1145/3543507.3583311.
[40] Tom Alby, *Popular, but hardly used: Has Google Analytics been to the detriment of Web Analytics?*, Proceedings of the 15th ACM Web Science Conference 2023 (Apr. 2023), https://dl.acm.org/doi/fullHtml/10.1145/3578503.3583601.
[41] Steven Englehardt et al., *Cookies That Give You Away: The Surveillance Implications of Web Tracking*, Proceedings of the 24th International Conference on World Wide Web (May 18, 2015), https://dl.acm.org/doi/10.1145/2736277.2741679.
[42] Panagiotis Papadopoulos et al., *Cookie Synchronization: Everything You Always Wanted to Know But Were Afraid to Ask*, Proceedings of the 28th International Conference on World Wide Web (May 2019), https://dl.acm.org/doi/abs/10.1145/3308558.3313542.
[43] Chris Mills, *Saying goodbye to third-party cookies in 2024*, Mozilla MDN (Dec. 7, 2023), https://developer.mozilla.org/en-US/blog/goodbye-third-party-cookies/.

that circumvent these controls. Commonly called "browser fingerprinting,"[44] these approaches identify unique combinations of characteristics of the user's device, including the web browser and extensions, screen resolution, local fonts, battery information, and hardware and software implementation of different browser APIs.[45] Recent studies have identified browser fingerprinting code on more than 25% of top websites.[46]

Internet service providers. Firms that provide internet access (commonly called "internet service providers") can monitor the traffic that customers send to collect information on consumers. While much web traffic is encrypted today, requests such as domain name system ("DNS") queries[47] and the setup of transport layer security ("TLS") connections (via Server Name Indication[48]) can reveal the domains to which consumers are connecting even if the traffic itself is encrypted. Even this limited view into traffic can be used to develop profiles of customers.

3.1.3 Data from mobile devices

The widespread popularity of mobile devices, including phones and tablets, has provided additional opportunities for collecting data on users.

Mobile apps. A distinguishing characteristic of mobile devices is that they allow third-party developers to run applications ("mobile apps") on users' devices. Commonly distributed through "app stores" run by the mobile operating system provider, these mobile apps can access information about the device's user including their geo-location, communication history, browsing data, identities of friends, and many other sensitive items. The variety and granularity of data that mobile apps can access has increased over time, and studies have found that mobile app privacy has generally deteriorated.[49] Today, popular mobile operating systems have privacy controls that allow users to select which data and services they wish to allow mobile apps to access, but app developers have been found to often make requests that over-provision their permissions,[50] and malicious developers have been found to circumvent privacy controls via side channels and other means.[51]

Third-party libraries. Mobile apps today are complex applications that interact with other services, such as analytics services and advertising networks. To implement these features, there are third-party libraries that

---

[44] Pierre Laperdrix et al., *Browser Fingerprinting: A Survey,* 14(2) ACM Transactions on the Web 1 (2020), https://dl.acm.org/doi/10.1145/3386040.

[45] Pouneh Nikkhah Bahrami et al., *FP-Radar: Longitudinal Measurement and Early Detection of Browser Fingerprinting.* 2022(2) Proceedings on Privacy Enhancing Technologies 557 (2022), https://petsymposium.org/popets/2022/popets-2022-0056.php.

[46] Umar Iqbal et al., *Fingerprinting the Fingerprinters: Learning to Detect Browser Fingerprinting Behaviors*, Proceedings of the 2021 IEEE Symposium on Security and Privacy 1143 (2021), https://www.computer.org/csdl/proceedings-article/sp/2021/893400a283/1mbmHGY5Lpu.

[47] Kevin Borgolte et al. *How DNS over HTTPS is Reshaping Privacy, Performance, and Policy in the Internet Ecosystem*, TPRC47: The 47th Research Conference on Communication, Information and Internet Policy (July 27, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3427563.

[48] Ghada Arfaoui et al., *The privacy of the TLS 1.3 protocol*, 2019(4) Proceedings on Privacy Enhancing Technologies 190 (2019), https://petsymposium.org/popets/2019/popets-2019-0065.php.

[49] Jingjing Ren et al., *Bug Fixes, Improvements, ... and Privacy Leaks A Longitudinal Study of PII Leaks Across Android App Versions*, Proceedings of the 2018 Network and Distributed System Security Symposium (2018), https://www.ndss-symposium.org/wp-content/uploads/2018/02/ndss2018_05B-2_Ren_paper.pdf.

[50] Eileen Pan et al., *Panoptispy: Characterizing Audio and Video Exfiltration from Android Applications*, 2018(4) Proceedings on Privacy Enhancing Technologies 33 (2018), https://petsymposium.org/popets/2018/popets-2018-0030.php.

[51] Joel Reardon et al., *50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System*, Proceedings of the 28th USENIX Security Symposium 603 (2019), https://www.usenix.org/system/files/sec19-reardon.pdf.

allow mobile app developers to easily integrate such services.[52] Such third-party libraries typically inherit the same permissions as the mobile app they are integrated into, and numerous apps have been found to integrate libraries that collect tracking information from users.[53] In fact, researchers have found that such third-party libraries can extract users' audio and video files, as well as create and exfiltrate screen recordings.[54] Recent studies have shown that tracking libraries from major providers are present in a significant fraction of popular mobile apps.[55]

Cross-device tracking. Consumers today often use multiple devices to access sellers' websites and services, including desktop computers, tablets, and mobile phones. Most tracking technologies are designed to track a specific device, so sellers are often interested in tracking *individuals* across multiple devices. Called "cross-device tracking,"[56] there are techniques that can link devices[57] based on login information to the same service, based on cookie syncing, or based on more advanced techniques such as ultrasonic signals.[58] Cross-device techniques can have significant implications for consumers, as it may violate their privacy expectations by linking together data they desired to keep separate.[59]

Mobile network providers. Mobile devices are often used via mobile (cellular) connections, meaning mobile network providers often have a detailed view of users' mobile web browsing and mobile app usage. Major network providers have been found to use customers' web browsing activity for advertising purposes.[60] Additionally, due to the nature of mobile networks, mobile network providers also can track users' course-grained locations. The Federal Communications Commission recently fined multiple major mobile network providers for illegally sharing customers' location data with "aggregators," who then resold that information to other location service providers.[61]

3.1.4 Data from other connected devices

Over the past few years, a robust ecosystem of internet-connected devices has developed, and many consumers have numerous devices throughout their home, their vehicle, and carried on their person.

---

[52] Xian Zhan et al., *Research on Third-Party Libraries in Android Apps: A Taxonomy and Systematic Literature Review*, 48(10) IEEE Transactions on Software Engineering 4181 (2021), https://ieeexplore.ieee.org/document/9542854/.
[53] Soteris Demetriou et al. *Free for All! Assessing User Data Exposure to Advertising Libraries on Android*, Proceedings of the 2016 Networks and Distributed Systems Security Symposium (2016), https://www.ndss-symposium.org/wp-content/uploads/2017/09/free-for-all-assessing-user-data-exposure-advertising-libraries-android.pdf.
[54] Eileen Pan et al., *Panoptispy: Characterizing Audio and Video Exfiltration from Android Applications*, 2018(4) Proceedings on Privacy Enhancing Technologies 33 (2018), https://petsymposium.org/popets/2018/popets-2018-0030.php.
[55] Konrad Kollnig et al., *Are iPhones Really Better for Privacy? A Comparative Study of iOS and Android Apps*, 2022(2) Proceedings on Privacy Enhancing Technologies 6 (2022), https://petsymposium.org/popets/2022/popets-2022-0033.php.
[56] Fed. Trade Comm'n, Cross-Device Tracking: An FTC Staff Report (Jan. 2017), https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf.
[57] Justin Brookman et al., *Cross-Device Tracking: Measurement and Disclosures*, 2017(2) Proceedings on Privacy Enhancing Technologies 133 (2017), https://petsymposium.org/popets/2017/popets-2017-0020.php.
[58] Nikolay Matyunin et al., *Zero-permission acoustic cross-device tracking,* Proceedings of the 2018 IEEE International Symposium on Hardware Oriented Security and Trust (2018), https://ieeexplore.ieee.org/abstract/document/8383887/.
[59] Sebastian Zimmeck et al., *A Privacy Analysis of Cross-device Tracking*, Proceedings of the 26th USENIX Security Symposium 1391 (2017), https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-zimmeck.pdf.
[60] Drew FitzGerald, *T-Mobile to Step Up Ad Targeting of Cellphone Customers*, *Wall St. J.,* Mar. 9, 2021, https://www.wsj.com/articles/t-mobile-to-step-up-ad-targeting-of-cellphone-customers-11615285803.
[61] Press Release, Fed. Comm. Comm'n, "FCC Fines Largest Wireless Carriers for Sharing Location Data" (Apr. 29, 2024), https://www.fcc.gov/document/fcc-fines-largest-wireless-carriers-sharing-location-data.

Because these devices are connected to the internet, they offer an additional mechanism for collecting data on users.

Internet-of-Things ("IoT") devices. IoT devices are increasingly commonplace. One common type of IoT device is "smart TVs", or televisions that embed applications (*e.g.*, to support streaming services). These devices have been shown to embed functionality designed to track users, transmitting viewing habits to third parties,[62] sometimes without users' knowledge or consent.[63] So-called "smart speakers" raise particular concerns, as they are designed to "listen in" on normal conversations and activate when particular phrases are spoken; research has shown that they can regularly mis-activate and record consumers' conversations.[64] Wearable "fitness trackers" have also been demonstrated to collect highly sensitive data on users, even leading to potential national security concerns.[65] And IoT devices have been used in concert with other devices to implement data collection: for example, developers were found to be using inaudible ultrasonic patterns in television advertisements, coupled with mobile apps that could receive those advertisements, to surreptitiously track which ads users were exposed to.[66]

Connected vehicles. Today, most vehicles sold in the U.S. are internet-connected via dedicated communications hardware using combinations of WiFi, mobile, and/or satellite networks. These vehicles have been called "smartphones on wheels," as they possess many of the same features as mobile devices, including cameras, microphones, GPS receivers, and support for third-party applications. As a result, the data that vehicles collect today, and how that data is used, raises a number of privacy concerns.[67] A recent review of the privacy policies of vehicle manufacturers found that the policies are very broad in scope: the policies state that vehicles can collect significant amounts of privacy-sensitive data, and that most manufacturers can share collected data with service providers, data brokers, and others.[68] And recent reporting has identified multiple car manufacturers that share driving behavior data from such connected cars with third parties that insurance companies use to inform the rates that potential buyers are offered,[69] as well as third parties that sell the granular information of individual vehicles.[70]

---

[62] Janus Varmarken et al., *The TV is Smart and Full of Trackers: Measuring Smart TV Advertising and Tracking*, 2020(2) Proceedings on Privacy Enhancing Technologies 129 (2020), https://petsymposium.org/popets/2020/popets-2020-0021.php.

[63] Press Release, Fed. Trade Comm'n, "VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent" (Feb. 16, 2017), https://www.ftc.gov/news-events/news/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it-collected-viewing-histories-11-million.

[64] Daniel J. Dubois et al., *When Speakers Are All Ears: Characterizing Misactivations of IoT Smart Speakers*, 2020(4) Proceedings on Privacy Enhancing Technologies 255 (2020), https://petsymposium.org/popets/2020/popets-2020-0072.php.

[65] Richard Perez-Pena & Matthew Rosenberg, *Strava Fitness App Can Reveal Military Sites*, N.Y. Times, Jan. 29, 2018, https://www.nytimes.com/2018/01/29/world/middleeast/strava-heat-map.html.

[66] Press Release, Fed. Trade Comm'n, "FTC Issues Warning Letters to App Developers Using 'Silverpush' Code" (Mar. 17, 2016), https://www.ftc.gov/news-events/news/press-releases/2016/03/ftc-issues-warning-letters-app-developers-using-silverpush-code.

[67] Fed. Trade Comm'n Staff in the Office of Technology and The Division of Privacy and Identity Protection, Cars & Consumer Data: On Unlawful Collection & Use (May 14, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/05/cars-consumer-data-unlawful-collection-use.

[68] Jen Caltrider et al., *It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy,* Mozilla *Privacy Not Included (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/.

[69] Kashmir Hill, *Automakers Are Sharing Consumers' Driving Behavior with Insurance Companies*, N.Y. Times, Mar. 11, 2024, https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html.

[70] Joseph Cox, *'Privacy Protecting' Car Location Data Seemingly Shows Where People Live, Work, and Go*, Vice, June 10, 2021, https://www.vice.com/en/article/car-location-data-not-anonymous-otonomo/.

3.1.5 Data from data brokers or other intermediaries

There are also companies whose primary business model is collecting, aggregating, sharing, and reselling consumers' personal data.[71] Frequently called "data brokers," these companies have existed since well before the advent of the internet.[72] Today, they collect data from a wide variety of sources—including government, commercial, and private records—and use it for a variety of purposes including identity verification, advertisement targeting, fraud detection, and credit estimation. Little direct study of data brokers exists, largely because they offer few user-facing tools that researchers can study; much of the research of the data collected by data brokers has used indirect sources such as partnerships with advertising platforms.[73]

3.2 Surveillance pricing outputs

Where might a consumer observe the impacts of surveillance pricing? The following is a brief overview of the literature and public reporting on surveillance pricing's *outputs*.

Prices offered. Sellers have historically determined their prices and the products offered based, at least in part, on who was buying. With surveillance pricing, sellers can use large-scale data—collected both by themselves and by third parties—coupled with advanced algorithms to help determine the prices they offer for their products.[74] Early studies of the surveillance pricing ecosystem have found that different consumers can be offered different prices for the same online product, depending on factors collected about the consumer such as their location,[75] the type of device they are browsing from,[76] or the language of their device.[77] These effects have been observed across industries, including transportation network companies,[78] online test preparation services,[79] office supply retailers,[80] broadband internet services,[81] and travel vendors.[82]

---

[71] Fed. Trade Comm'n, Data Brokers: A Call for Transparency and Accountability (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.
[72] Natasha Singer, *Mapping, and Sharing, the Consumer Genome*, N.Y. Times, June 16, 2012, https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html
[73] Giridhari Venkatadriet al., *Auditing Offline Data Brokers via Facebook's Advertising Platform*, *in* Proceedings of the 28th International Conference on World Wide Web 1920 (May 2019), https://dl.acm.org/doi/abs/10.1145/3308558.3313666.
[74] Le Chen et al., *An Empirical Analysis of Algorithmic Pricing on Amazon Marketplace*, *in* Proceedings of the 25th International Conference on World Wide Web 1339 (Apr. 2012), https://dl.acm.org/doi/10.1145/2872427.2883089.
[75] Jakub Mikians et al., *Detecting price and search discrimination on the internet*, *in* Proceedings of the 11th ACM workshop on Hot Topics in Networks 79 (Oct. 2012), https://dl.acm.org/doi/10.1145/2390231.2390245.
[76] Aniko Hannak et al., *Measuring Price Discrimination and Steering on E-commerce Web Sites*, *in* Proceedings of the 2014 ACM Internet Measurement Conference 305 (Nov. 2014), https://dl.acm.org/doi/10.1145/2663716.2663744.
[77] Thomas Hupperich et al., *An Empirical Study on Online Price Differentiation*, *in* Proceedings of the 8th ACM Conference on Data and Application Security and Privacy 76 (Mar. 2018), https://dl.acm.org/doi/10.1145/3176258.3176338.
[78] Le Chen et al., *Peeking Beneath the Hood of Uber*, *in* Proceedings of the 2015 ACM Internet Measurement Conference 495 (Oct. 2015), https://dl.acm.org/doi/10.1145/2815675.2815681.
[79] Kenyon Vafa et al., *Price Discrimination in The Princeton Review's Online SAT Tutoring Service*, Technology Science 2015090101, Aug. 31, 2015, https://techscience.org/a/2015090102/.
[80] Jennifer Valentino-DeVries et al., *Websites Vary Prices, Deals Based on Users' Information*, Wall St. J., Dec. 24, 2012, https://www.wsj.com/articles/SB10001424127887323777204578189391813881534.
[81] Leon Yin & Aaron Sankin, *Dollars to Megabits, You May Be Paying 400 Times As Much As Your Neighbor for Internet Service,* The Markup (Oct. 19, 2022, https://themarkup.org/still-loading/2022/10/19/dollars-to-megabits-you-may-be-paying-400-times-as-much-as-your-neighbor-for-internet-service.
[82] Jakub Mikians et al., *Detecting price and search discrimination on the internet*, *in* Proceedings of the 11th ACM workshop on Hot Topics in Networks 79 (Oct. 2012), https://dl.acm.org/doi/10.1145/2390231.2390245.

Targeted discounts. Sellers can implement surveillance pricing strategies via coupons or discount codes,[83] often delivered directly to potential buyers via mobile applications.[84] This approach enables the "nominal" price for a given good or service to stay constant across all potential buyers, while also enabling potential additional tracking and data collection via the coupon code (which can, for example, include additional information about how the potential buyer found the coupon). With much commerce happening via mobile applications, sellers can also use those apps to push tailored offers to customers, such as offering fewer discounts right after a customer's payday, or offering differently-priced products or coupons during times when the customer's budget is tighter.[85]

Products offered. Other studies have examined how different users are shown different sets of products or services, based on information that is collected about them. This can happen either when directly visiting a seller's site[86] or via advertisements.[87] Commonly called "steering," examples of this practice have been observed in the hotel industry,[88] and some have claimed it has happened on e-commerce platforms.[89] Many e-commerce platforms provide recommendations for products for a potential buyer to consider, and those recommendations have been shown to depend on both data about the potential buyer, as well as the e-commerce platforms' preferences for promoting their own retail products.[90]

Advertisements. Because the surveillance pricing ecosystem relies heavily on data from online advertising and tracking, consumers may frequently notice its effects in which advertisements they are shown online as advertisements can be used by sellers to call potential buyers' attention to particular items. These can include ads targeted to vulnerable populations,[91] ads with content and images algorithms have predicted consumers are more likely to engage with,[92] and ads for products the consumer previously viewed but did not purchase.[93]

4 Potential surveillance pricing harms

The rise of the surveillance pricing ecosystem, enabled by the robust collection of consumer data, can, for

---

[83] Lydia DePillis, *Consumers Hate 'Price Discrimination,' but They Sure Love a Discount*, *N.Y. Times,* Apr. 6, 2024, https://www.nytimes.com/2024/04/06/business/economy/wendys-company-price-discrimination.html.
[84] David Dayen, *One Person One Price*, The American Prospect (June 4, 2024), https://prospect.org/economy/2024-06-04-one-person-one-price/.
[85] *Plexure and McDonald's: Revolutionizing Personalized Experiences.*, Tepia, https://tepia.co/plexure-and-mcdonalds-revolutionizing-personalized-experiences/ (last visited Jan. 9, 2025).
[86] Aniko Hannak et al., *Measuring Price Discrimination and Steering on E-commerce Web Sites*, *in* Proceedings of the 2014 ACM Internet Measurement Conference 305 (Nov. 2014), https://dl.acm.org/doi/10.1145/2663716.2663744.
[87] Vincent Toubiana, *A look at the use of « Ethnic Affinities » by advertisers*, Laboratoire d'Innovation Numérique de la CNIL, Feb. 13, 2017, https://linc.cnil.fr/look-use-ethnic-affinities-advertisers.
[88] Dana Mattioli, *On Orbitz, Mac Users Steered to Pricier Hotels*, Wall St. J., Aug. 23, 2012, https://www.wsj.com/articles/SB10001424052702304458604577488822667325882.
[89] Ashley Belanger, *Amazon hides cheaper items with faster delivery, lawsuit alleges*, Ars Technica, Feb. 12, 2024, https://arstechnica.com/tech-policy/2024/02/amazons-algorithm-deliberately-hides-the-best-deals-lawsuit-claims/.
[90] Nan Chen & Hsin-Tien Tiffay Tsai, *Steering via Algorithmic Recommendations*, RAND J. of Econ., Forthcoming, (Apr. 25, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3500407.
[91] Tinhinane Medjkoune et al., *Marketing to Children Through Online Targeted Advertising: Targeting Mechanisms and Legal Aspects*, *in* Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security 180 (Nov. 2023), https://dl.acm.org/doi/10.1145/3576915.3623172.
[92] Levi Kaplan et al., *Measurement and analysis of implied identity in ad delivery optimization*, in Proceedings of the 22nd ACM Internet Measurement Conference 195 (Oct. 2022), https://dl.acm.org/doi/10.1145/3517745.3561450.
[93] Muhammad Bashir et al., *Tracing Information Flows Between Ad Exchanges Using Retargeted Ads*, *in* Proceedings of the 25th USENIX Security Symposium 481 (2016), https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_bashir.pdf.

instance, violate consumers' privacy through both inferred attributes that consumers may wish to not reveal[94] as well as inadvertent data leaks that can affect hundreds of millions of Americans.[95] But the potential harms of surveillance pricing are not limited to data collection: in the quest for maximizing returns, the decisions made by surveillance pricing systems can discriminate to the detriment of historically disadvantaged groups. The use of common data and algorithms by multiple sellers to set offers and prices also raises new competition concerns. Each of these are described in more detail below.

4.1 Harms to consumers

Surveillance pricing can impact consumers in a variety of ways, including direct effects on the prices, products, and opportunities they are presented with when interacting with sellers, as well as longer-term effects on their privacy.

Prices and Promotions. One of the goals of surveillance pricing algorithms is to predict potential buyers' willingness to pay for a given product or service, as sellers who can make such predictions may be able to increase their profits. There are concerns that, at least for some potential buyers, the use of surveillance pricing may result in some consumers paying higher prices than others in cases where the algorithms predict the potential buyer has a strong desire for the given product or service.[96] More broadly, there is a concern that the use of surveillance pricing may reduce consumer surplus overall by extracting more from certain buyers.[97] Other public reporting has flagged illusory markdowns, promotions or "constant sales,"[98] where some retailers "mark up the prices and then offer seemingly deep discounts to make the deals look more attractive."[99] Using surveillance pricing tools to deploy illusory or deceptive promotions through targeted pricing may risk harming consumers.

Privacy. Many first and third parties collect online and offline information on consumers for purposes that include targeted advertising, analytics, and surveillance pricing. Such large-scale collection of data can pose significant privacy risks for consumers, including when firms infer information that consumers may wish to keep private, and the unauthorized disclosure of information to third-parties. Examples of ways in which large scale data collection can negatively impact consumers include sensitive collected data (*e.g.*, data collected by menstrual tracking apps) being shared with third parties,[100] data that can enable physical harm by stalkers,[101] and even risks to national security through the sale of data on U.S. military personnel.[102]

---

[94] Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. Times Magazine, Feb. 16 ,2012, https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.
[95] Fed. Trade Comm'n, Equifax Data Breach Settlement (Nov. 2024), https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement.
[96] David Dayen, *The Emerging Danger of Surveillance Pricing,* Jacobin (July 9, 2024), https://jacobin.com/2024/07/surveillance-personalized-pricing-data-collection.
[97] Jean-Pierre Dubé & Sanjog Misra, *Personalized Pricing and Consumer Welfare*, 131(1) J. of Political Econ. 131 (2023), https://www.journals.uchicago.edu/doi/abs/10.1086/720793.
[98] Kevin Brasler, *Spend less this holiday shopping season by outsmarting common sales strategies*, Minn. Star Trib., Nov. 2, 2024, https://www.startribune.com/holiday-shopping-sales-strategies-common-mistakes-retailer-gift/601173610.
[99] Jaclyn Peiser, *A common, illegal tactic retailers use to lure consumers*, Wash. Post, Nov. 21, 2023, https://www.washingtonpost.com/business/2023/11/21/fake-sale-deceptive-pricing/.
[100] Drew Harwell, *Is Your Pregnancy App Sharing Your Intimate Data with Your Boss?*, Wash. Post, Apr. 10, 2019, https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/.
[101] Rohit Chopra, Director, Consumer Financial Protection Bureau, Prepared Remarks on Protecting Americans from Harmful Data Broker Practices (Dec. 3, 2024), https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-of-cfpb-director-rohit-chopra-on-protecting-americans-from-harmful-data-broker-practices/.
[102] Justin Sherman et al., Data Brokers and the Sale of Data on US Military Personnel, (Nov. 2023), https://techpolicy.sanford.duke.edu/data-brokers-and-the-sale-of-data-on-us-military-personnel/.

Additionally, the large-scale aggregation of sensitive data on consumers means that the data sets that are collected are attractive targets for malicious actors. In fact, some of the largest data breaches—affecting hundreds of millions of Americans—have been due to large-scale data aggregators.[103]

Data collection obfuscation. One of the key criticisms of the data collected for purposes including surveillance pricing and targeted advertising is the obfuscation by companies of their data collection practices and activities.[104] The Director of the FTC's Consumer Protection Bureau has stated, "Americans are not reading every word of every privacy policy [and even if we did] it would be difficult to comprehend the full extent of how [data] can be used. And even if we read the policies *and* understood them, we can hardly exercise choice given how much we rely on digital services[.]"[105] This lack of notice or control is particularly concerning as it affords the opportunity for sellers to use the collected data to the detriment of vulnerable populations: for example, advertisers have been shown to target potential buyers in ways that are potentially predatory,[106] such as by targeting individuals who suffer from gambling addiction with casino ads.[107]

Techniques have been proposed to provide consumers with control over when data is collected but have seen little adoption. For example, the "Do Not Track" setting for web browsers[108] offered the promise for consumers to state that they did not wish to have their data collected as they browsed the web. Unfortunately, due to lack of wide-scale adoption,[109] this feature has now been deprecated in major browsers.[110] In certain jurisdictions in the U.S., consumers have certain legal rights to request information about the data collected about them and request it be deleted,[111] but similar legal rights do not yet exist at the federal level.

Discrimination. Studies have also demonstrated how the use of data on consumers combined with AI-powered algorithms in other contexts—such as in online advertising—can result in discrimination in access to housing[112] and employment opportunities.[113] In fact, some platforms have agreed to change their

---

[103] Fed. Trade Comm'n, Equifax Data Breach Settlement (Nov. 2024), https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement.

[104] Stefan Larsson et al., *Notified but Unaware: Third-party Tracking Online*, 8(1) Critical Analysis of Law 101 (2021), https://cal.library.utoronto.ca/index.php/cal/article/view/36282.

[105] Samuel Levine, Director, Bureau of Consumer Protection, Fed. Trade Comm'n, Prepared Remarks: Toward a Safer, Freer, and Fairer Digital Economy (Apr. 17, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/20240417-Reidenberg-Lecture-final-for-publication-Remarks-Sam-Levine.pdf..

[106] Shanti Das, *Google profiting from 'predatory' loan adverts promising instant cash,* The Guardian*,* Mar. 13, 2022, https://www.theguardian.com/technology/2022/mar/13/google-profiting-from-predatory-loan-adverts-promising-instant-cash.

[107] Rob Davies, *Online casino advert banned for targeting problem gamblers,* The Guardian*,* Oct. 9, 2022, https://www.theguardian.com/society/2019/oct/09/casumo-ad-banned-for-targeting-people-trying-to-stop-gambling.

[108] Julia Angwin, *Web Tool On Firefox To Deter Tracking*, Wall St. J., Jan. 21, 2011, https://www.wsj.com/articles/SB10001424052748704213404576100441609997236.

[109] Kashmir Hill, *'Do Not Track,' the Privacy Tool Used by Millions of People, Doesn't Do Anything*, Gizmodo*,* Oct. 15, 2019, https://gizmodo.com/do-not-track-the-privacy-tool-used-by-millions-of-peop-1828868324.

[110] Glenn Fleishman, *How the tragic death of Do Not Track ruining the web for everyone*, Fast Company, Mar. 17, 2019, https://www.fastcompany.com/90308068/how-the-tragic-death-of-do-not-track-ruined-the-web-for-everyone.

[111] Office of the Attorney General, State of California Dep't of Justice, California Consumer Privacy Act (CCPA), Mar. 13, 2025, https://oag.ca.gov/privacy/ccpa/.

[112] Joshua Asplund et al., *Auditing Race and Gender Discrimination in Online Housing Markets*, 14(1) Proceedings of the International AAAI Conference on Web and Social 24 (May 2020), https://ojs.aaai.org/index.php/ICWSM/article/view/7276.

[113] *See* Anja Lambrecht & Catherine Tucker, *Algorithmic Bias? An Empirical Study of Apparent Gender-Based Discrimination in the Display of STEM Career Ads*, , 65(7) Management Science 2966 (2019), https://pubsonline.informs.org/doi/10.1287/mnsc.2018.3093; Basileal Imana et al., *Auditing for Discrimination in Algorithms Delivering Job Ads*, *in* Proceedings of the 30th International Conference on World Wide Web 3767 (Apr. 2021), https://dl.acm.org/doi/10.1145/3442381.3450077.

systems[114] after their algorithms were claimed to lead to potentially discriminatory outcomes for some opportunity ads.[115] The surveillance pricing ecosystem can rely on similar data and algorithmic infrastructure as these systems, and similar concerns may arise if pricing uses protected consumer characteristics such as race or sex.[116]

Impacts to other businesses. Many of the same concerns outlined above hold for business-to-business markets, where businesses that are buying a product or service may be similarly impacted. Notable examples of industries where this has been observed include online recruiting,[117] where sellers have been found to set the price of the service based on characteristics of the perceived willingness of the buyer firm to pay.

4.2 Harms to competition

Competing sellers employing surveillance pricing algorithms may also generate pricing that is actually or effectively collusive. The algorithms firms use to set prices may end up coordinating their prices as if the firms had directly colluded.[118] Alternatively, multiple sellers might rely on common data or algorithms (*e.g.*, via pricing recommendations provided by third-party services[119]), which may again lead to potentially collusive pricing outcomes. Multiple sellers agreeing to rely on the same algorithm to make pricing decisions or to provide competitively-sensitive, non-public information to a common third-party provider of pricing services may constitute an anticompetitive agreement to coordinate prices or exchange information.[120] The FTC has noted that a price-fixing agreement is still unlawful regardless of whether the conspirators enforce compliance with the illegal agreement or retain some pricing discretion to depart from the fixed prices.[121] For example, the Department of Justice in *U.S. v. RealPage*,[122] alleges that landlords' agreements to provide RealPage with access to nonpublic rental transaction data and to use RealPage's rental pricing software harms the competitive process and renters. There are a number of other legal cases—some of which are still ongoing—concerning the competitive impacts of agreements to use algorithmic pricing, including in the hotel

[114] Press Release, Dep't of Justice, "Justice Department Secures Groundbreaking Settlement Agreement with Meta Platforms, Formerly Known as Facebook, to Resolve Allegations of Discriminatory Advertising," (June 21, 2022), https://www.justice.gov/opa/pr/justice-department-secures-groundbreaking-settlement-agreement-meta-platforms-formerly-known.
[115] Muhammed Ali et al., *Discrimination through Optimization: How Facebook's Ad Delivery Can Lead to Biased Outcomes*, 3 Proceedings of the ACM on Human-Computer Interaction 1 (Nov. 2019), https://dl.acm.org/doi/10.1145/3359301.
[116] Fed. Trade Comm'n, Personalized Pricing in the Digital Era – Note by the United States, (Nov. 28, 2018), https://www.ftc.gov/system/files/attachments/us-submissions-oecd-2010-present-other-international-competition-fora/personalized_pricing_note_by_the_united_states.pdf.
[117] Jean-Pierre Dubé & Sanjog Misra, *Personalized Pricing and Consumer Welfare*, 131(1) J. of Political Econ. 131 (2023), https://www.journals.uchicago.edu/doi/abs/10.1086/720793.
[118] Aneesa Mazumdar, *Note: Algorithmic Collusion*, 122(2) Columbia Law Review 449 (2022), https://columbialawreview.org/content/algorithmic-collusion-reviving-section-5-of-the-ftc-act/.
[119] *See* Blooomreach, How to Personalize Offers Based on Customer Preferences With Contextual Personalization, https://www.bloomreach.com/en/library/use-cases/personalize-offers-based-on-customer-preferences-with-contextual-personalization (last visited Jan. 9, 2025); PROS, Develop impactful pricing strategies with cutting-edge AI, https://pros.com/products/price-optimization-software/ (last visited Jan. 9, 2025).
[120] Press Release, Dep't of Justice, "Justice Department Sues RealPage for Algorithmic Pricing Scheme that Harms Millions of American Renters" (Aug. 23, 2024), https://www.justice.gov/opa/pr/justice-department-sues-realpage-algorithmic-pricing-scheme-harms-millions-american-renters.
[121] Dep't of Justice and Fed. Trade Comm'n, Statement of Interest The United States of America, Duffy v. Yardi, 2:23-cv-01391 (W.D. Wash. Mar. 1, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/YardiSOI-filed%28withattachments%29_0.pdf.
[122] Press Release, Dep't of Justice, "Justice Department Sues RealPage for Algorithmic Pricing Scheme that Harms Millions of American Renters" (Aug. 23, 2024), https://www.justice.gov/opa/pr/justice-department-sues-realpage-algorithmic-pricing-scheme-harms-millions-american-renters.

industry[123] and with regard to consumer goods.[124] In addition, even without using common algorithms, there are concerns that the growing use of pricing algorithms can potentially threaten competition,[125] lead to collusive strategies,[126] and raise prices.[127] Surveillance pricing may add additional dimensions to these concerns.

5 Areas for Further Research

As highlighted above, there is much to explore about surveillance pricing, ranging from questions about how data is collected, to how that data is used, to how surveillance pricing is harming consumers and the marketplace. FTC staff hope that many of these questions will be addressed by the ongoing 6(b) study, and also recognizes the value of further academic research. Specific directions for fruitful future research include:

Understanding implications of surveillance pricing. Before surveillance pricing, sellers would choose a price for a good or service and potential buyers would choose whether to accept it. Thus, potential buyers who had a higher "willingness to pay" would end up paying less than they might be willing to. One of the goals of surveillance pricing is to use collected data to better estimate a given potential buyer's willingness to pay, and then customize the price based on that estimate. Thus, more work is needed to understand whether and when surveillance pricing results in higher prices for consumers, and how surveillance pricing impacts information asymmetries between potential buyers (who observe their own experience) and sellers (who have data on potentially millions of other buyers and can work with third parties who may have data on many more).

Understanding effects of discounts and coupons. One common mechanism for implementing surveillance pricing is via discounts or coupons, which are personalized to the potential buyer.[128] The net effect of such an approach, taken to the limit, is that every potential buyer receives a different effective price, even if a nominal price exists. This raises concerns about "reference pricing" and whether claims such as "up to 25% off" might be unfair or deceptive: if no actual potential buyer would pay the nominal price, is it accurate for a seller to advertise such a discount? More research into the larger effects of surveillance pricing is needed to understand these impacts.

Measuring consumer impacts. As highlighted above, measuring the impacts of surveillance pricing is a time-consuming and laborious task for researchers, who often must recruit representative samples of participants for studies including both surveys[129] and empirical measurements of what data real-world systems collect. There is an opportunity to amortize this cost across many researchers through the creation of

---

[123] Press Release, Fed. Trade Comm'n, "FTC and DOJ File Statement of Interest in Hotel Room Algorithmic Price-Fixing Case" (Mar. 28, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/03/ftc-doj-file-statement-interest-hotel-room-algorithmic-price-fixing-case

[124] Press Release, Dep't of Justice, "Online Retailer Pleads Guilty for Fixing Prices of Wall Posters" (Aug. 11, 2016), https://www.justice.gov/opa/pr/online-retailer-pleads-guilty-fixing-prices-wall-posters.

[125] The New Invisible Hand? The Impact of Algorithms on Competition and Consumer Rights: Hearing Before U.S. Senate, Comm. on the Judiciary, Subcomm. on Competition Policy, Antitrust, and Consumer Rights, 118 Cong. (2023) (Statement of Bill Baer), https://www.brookings.edu/wp-content/uploads/2023/12/GS_12132023_testimony_bill-baer.pdf.

[126] Emilio Calvano et al., *Artificial Intelligence, Algorithmic Pricing, and Collusion*, 110(10) Am. Econ. Rev. 3267, 3297 (2020). https://www.aeaweb.org/articles?id=10.1257/aer.20190623

[127] Zach Y. Brown & Alexander MacKay, *Competition in Pricing Algorithms*, 15(2) American Econ. J.: Microeconomics 109, 156 (2023). https://www.aeaweb.org/articles?id=10.1257/mic.20210158

[128] Minh Thi Thuy Nguyen et al., *A Systematic Review on the Effects of Personalized Price Promotions for Food Products*, 25(3) J. Food Products Marketing 257, 275 (2019). https://www.tandfonline.com/doi/abs/10.1080/10454446.2018.1529647

[129] Martin Spann et al., "Algorithmic Pricing: Implications for Consumers, Managers, and Regulators" (Nat'l Bureau of Econ. Rsch., Working Paper No. 32540, Jun. 2024). https://www.nber.org/papers/w32540.

common sets of participants who have already been "on boarded" and can choose to participate in different studies. Models for such an approach exist in other domains[130] and could be tailored to understand the impacts of surveillance pricing as well.

Understanding impacts on competition. Sellers agreeing to use the same algorithm to determine prices may lead to reduced rivalry and/or the ability to increase prices,[131] but the limits of when the use of common *data* to independently build algorithms might result in similar effects are not yet known. This is especially relevant as the behavior of modern AI systems is often heavily driven by the data they are trained on. In other words, what happens if multiple sellers use the same data to develop separate algorithms for deciding prices, and those algorithms all end up with substantially similar behavior?

Additionally, more research is needed to understand the extent to which use of surveillance pricing strategies commonly involves or promotes the use of either common pricing algorithms and/or common data sets, across competing firms. As discussed above, sellers in the surveillance pricing ecosystem can amass granular customer data from a variety of common sources, presumably without resorting to potentially anticompetitive information exchanges. Existing studies on the competitive impact of algorithmic pricing suggest that its adoption may lead to supra-competitive pricing, even without agreements to use common algorithms or data; but this body of research is in its infancy. As sellers become increasingly sophisticated in how they gather customer information and deploy pricing algorithms in the surveillance pricing ecosystem, additional research is needed into the impacts of autonomous pricing algorithms on pricing and the competitive process.

[130] *Helping researchers understand online behavior.,* National Internet Observatory. https://nationalinternetobservatory.org/ (last visited Jan. 9, 2025).
[131] Hannah Garden-Monheit & Ken Merber. *Price fixing by algorithm is still price fixing,* FTC Business Blog (Mar. 1, 2024), https://www.ftc.gov/business-guidance/blog/2024/03/price-fixing-algorithm-still-price-fixing.