

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER
to the
FEDERAL TRADE COMMISSION AND U.S. DEPARTMENT OF JUSTICE'S ANTITRUST
DIVISION

Re: Joint Public Inquiry for Consideration of Guidance on Business Collaborations

Docket No. ATR-2026-0001

May 21, 2026

The Electronic Privacy Information Center (EPIC) submits these comments in response to the Federal Trade Commission (FTC or Commission) and U.S. Department of Justice's (DOJ) Antitrust Division's joint public inquiry seeking information regarding potential guidance on collaboration among competitors.¹ EPIC asks that the Agencies consider privacy protections when guiding the market on antitrust law and policy. While business collaborations and joint ventures can benefit the economy, there are potential risks that harm consumers when businesses consolidate data without adequate safeguards in place. Today's data economy that deploys ubiquitous surveillance and emerging unregulated technologies require that the Agencies consider the privacy implications of joint ventures on consumers in the reintroduction of guidance on business collaborations. Privacy and competition play a vital role in a thriving economy, and the American people benefit when there are strong data privacy safeguards in place.

¹ DOJ and FTC Seek Public Comment for Guidance on Business Collaborations, Docket No. ATR-2026-0001 (Feb. 23, 2026), <https://www.regulations.gov/docket/ATR-2026-0001/document>.

EPIC is an independent, nonpartisan public interest research center in Washington, D.C., established in 1994 to protect privacy, freedom of expression, and democratic values in the information age.² For decades, EPIC has worked under different administrations to safeguard individuals' personal data and to protect consumer privacy. EPIC focuses public attention on emerging consumer privacy issues, including the growing consolidation of market power in the technology industry and how it impacts competition.³ EPIC has long urged the FTC to assess consumer privacy impacts when reviewing proposed mergers between companies that control, collect, process, disclose, or retain personal information.⁴ EPIC recommends that: (1) the Agencies prioritize data privacy in considering guidance; (2) the Agencies provide robust protections against surveillance-driven personalized pricing in any guidance; and (3) the Agency establish guidance that underscores the crucial role of privacy in competition.

I. Any Guidance that the Agencies Publish Must Include Data Privacy Protections

The Agencies should prioritize data privacy when considering guidance for business collaborations because data is a large part of companies' collaborations and joint ventures, but companies often misuse and fail to protect personal data. Online firms over collect and commodify swaths of consumer data which deprives consumers of control over their personal information, heightens security risks, and leads to misuse, manipulation, and discrimination. Notably, privacy risks increase when businesses collaborate on joint ventures because they combine, transfer, merge, and match the respective business' data. These risks can be mitigated by incorporating privacy protective practices like data minimization.

² EPIC, *About Us* (2026), <https://epic.org/about/>.

³ EPIC, *Competition and Privacy* (2026), <https://epic.org/issues/consumer-privacy/competition-and-privacy/>.

⁴ See e.g., Comments of EPIC, Assessment of the FTC's Prior Actions on Merger Review and Consumer Privacy, FTC, FTC File No. P143100 (Mar. 17, 2015), <https://epic.org/wp-content/uploads/privacy/internet/ftc/Merger-Remedy-3-17.pdf>; Comments of EPIC, On Request for Comment Regarding Draft Merger Guidelines, FTC, FTC-2023-0043-0001 (Sep. 18, 2023), <https://epic.org/documents/comments-of-epic-on-ftc-and-doj-draft-merger-guidelines/>.

Privacy protective guidance on business collaborations must include data minimization standards to best promote competition and protect consumers. Data minimization is a standard that limits a business' collection, use, transfer, and retention of consumer's data to what is reasonably necessary and proportionate to fulfill a product or service for a consumer.⁵ Data minimization is the most effective tool for protecting consumer privacy, safeguarding personal information, and aligning commercial data practices to consumer expectations. EPIC has written extensively on the importance of data minimization and has long agreed with the FTC's position that the overcollection and misuse of personal information is a widespread problem that harms millions of consumers every day.⁶ In 2022, EPIC submitted substantial comments concerning the FTC's proposed rulemaking on commercial surveillance, urging the Commission to establish a data minimization standard that would be consistent with consumer expectation.⁷ This is especially important when companies transfer consumers' personal information in a collaboration or joint venture. A consumer may expect that a company with which they are interacting directly would collect their data, but they would not expect that this company would disclose it to a different, unknown company. EPIC has long advocated for a data minimization rule that would prohibit all secondary uses with limited

⁵ EPIC, *Data Minimization* (2026), <https://epic.org/issues/consumer-privacy/data-minimization/>.

⁶ Comments of EPIC, *Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem*, FTC, Proposed Trade Regulation Rule on Commercial Surveillance & Data Sec., Commercial Surveillance ANPR, R111004 at 30 (Nov. 2022), <https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf>; *see e.g.*, John Davisson, *Data Minimization: A Pillar of Data Security, But More Than That Too*, EPIC (June 23, 2023), <https://epic.org/data-minimization-a-pillar-of-data-security-but-more-than-that-too/>; Sara Geoghegan, *Data Minimization: Limiting the Scope of Permissible Data Uses to Protect Consumers*, EPIC (May 4, 2024), <https://epic.org/data-minimization-limiting-the-scope-of-permissible-data-uses-to-protect-consumers/>; *see generally* EPIC, *Data Minimization* (2026), <https://epic.org/issues/consumer-privacy/data-minimization/>.

⁷ Comments of EPIC, *EPIC Comments, Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem*, FTC, Proposed Trade Regulation Rule on Commercial Surveillance & Data Sec., Commercial Surveillance ANPR, R111004 (Nov. 2022), <https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf>.

exceptions⁸ because commercial surveillance practices subvert the ability of consumers to make meaningful, informed decisions in the marketplace.⁹ Current standard business practices, including joint collaborations, benefit from a user-centered approach of data minimization and the Agencies should adopt that standard in any guidance they put forth.

II. Guidance that Limits Algorithmic Pricing Would Reduce Consumer Harms

Algorithmic pricing is an emerging business practice that the 2000 Collaboration Guidelines do not address.¹⁰ The Agencies should consider providing additional guidance to limit data practices that fuel algorithmic pricing because the practice raises data privacy, price discrimination, and transparency concerns. Companies have access to vast troves of personal data about consumers and advanced AI systems that they use to infer how much a consumer is willing to pay, benefitting the company to the detriment of consumers. When businesses collaborate, they can transfer data and this data can feed algorithms that set prices higher for consumers. People have no idea that a system is using their data to set a price for them and can lead to consumers being unfairly exploited and deceived.¹¹ When businesses that engage in algorithmic pricing merge or collaborate, the data privacy risks exacerbate.

The Agencies' guidance should provide protections for consumers when business collaborations use consumers' personal information in algorithmic pricing because this practice may

⁸ See EPIC and Consumer Reports, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking* (Jan. 26, 2022), https://epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDDataMinimization_012522_VF_.pdf.

⁹ Suzanne Bernstein, *Data Minimization: Centering Reasonable Consumer Expectation in the FTC's Commercial Surveillance Rulemaking*, EPIC (Apr. 30, 2023), <https://epic.org/data-minimization-centering-reasonable-consumer-expectation-in-the-ftcs-commercial-surveillance-rulemaking/>.

¹⁰ See FTC and DOJ, *Antitrust Guidelines for Collaborations Among Competitors* (Apr. 2000), https://www.ftc.gov/sites/default/files/documents/public_events/joint-venture-hearings-antitrust-guidelines-collaboration-among-competitors/ftcdojguidelines-2.pdf [hereinafter "2000 Collaboration Guidelines"].

¹¹ Press Release, Erik Nasarenko, Ventura County District Attorney, Target Corporation to Pay \$5 Million in Price Accuracy Settlement (Mar. 11, 2022), <https://www.vcdistrictattorney.com/wp-content/uploads/2022/03/22-017-Target-Corporation-Reid-Settlement.pdf>.

harm consumers and guidelines would provide a level playing field for all businesses. For example, EPIC highlighted Kroger's algorithmic pricing harms in light of media attention over Kroger's potential use of facial recognition to enhance its algorithmic pricing capabilities and its use of electronic shelving labels to profile and target customers with higher prices.¹² In February 2026, EPIC and a coalition of national consumer protection and privacy groups called on the FTC to initiate a rulemaking that would require companies to disclose when they are using algorithmic pricing.¹³ The letter explains why algorithmic pricing poses widespread harms to consumers, provides real-life examples of companies engaging in these practices, and describes how clear federal guidelines around algorithmic pricing could level the playing field for businesses. Guidance on commonsense, basic disclosures for algorithmic pricing and limits on data uses would promote consumer choice and prevent companies from engaging in unfair and deceptive practices.

The group also urged the FTC to complete its Section 6(b) study surveillance pricing, which aligns with FTC Chair Andrew Ferguson's position that a final comprehensive report should be completed.¹⁴ Completing its Section 6(b) study on surveillance pricing would help inform any additional guidance on business collaborations. The Agencies should consider how business collaborations use data in algorithmic pricing in their guidance so businesses can avoid harmful, discriminatory, or collusive pricing practices.

¹² Mayu Tobin-Miyaji, *Kroger's Surveillance Pricing Harms Consumers and Raises Prices, With or Without Facial Recognition*, EPIC (Feb. 15, 2025) <https://epic.org/krogers-surveillance-pricing-harms-consumers-and-raises-prices-with-or-without-facial-recognition/>.

¹³ Comments of EPIC et al., Petition for Rulemaking of Andrew Gonzalez Re: Disclosure of Artificial Intelligence Systems for Commercial Profiling and Price Manipulation, FTC, Docket No. FTC-2026-0034 (Feb. 23, 2026), https://epic.org/wp-content/uploads/2026/02/Consumer-and-Law-Student-Groups_Personalized-Algorithmic-Pricing-Public-Comment_2-23-26.pdf

¹⁴ See Public Statement, Andrew N. Ferguson, Chairman, FTC, Dissenting Statement of Commissioner Andrew N. Ferguson Joined by Commissioner Melissa Holyoak Regarding the Surveillance Pricing 6(b) Staff Research Summaries Matter Number P246202 (Jan. 17, 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/surveillance-pricing-6b-research-summaries-ferguson-dissent-final.pdf.

III. The Agencies Must Consider Privacy Implications in Market Consolidation and Competition Remedies

The American people and economy can benefit from business collaborations when strong data privacy is baked in. The Agencies should emphasize that data privacy protections must be a priority when business collaborators exchange data. One of the key goals of the 2000 Guidelines was to deter “collaborations likely to harm competition and consumers.”¹⁵ EPIC has long advocated that privacy and competition go hand in hand.¹⁶ In several comments to the Consumer Financial Protection Bureau, EPIC highlighted ways to best protect consumer data, including when companies transfer data.¹⁷ EPIC explained that portability, interoperability, and data transfers implicated by competitor collaborations are only tolerable if paired with strict data minimization standards, strong data security protocols, secondary use restrictions, limits on third party access, and data retention rules. EPIC also advocates for stronger consumer rights over their data, including providing consumers with easy ways to revoke third-party access to their data from both sides of the collaborative arrangement as well as deletion rights. The Agencies should include guidance on reasonable third-party access revocation methods so consumers have individual data autonomy and can protect themselves from harms that stem from unsecure data transfers.

¹⁵ See generally FTC and DOJ, Antitrust Guidelines for Collaborations Among Competitors 2 (Apr. 2000), https://www.ftc.gov/sites/default/files/documents/public_events/joint-venture-hearings-antitrust-guidelines-collaboration-among-competitors/ftcdojguidelines-2.pdf [hereinafter “2000 Collaboration Guidelines”].

¹⁶ EPIC, *Competition and Privacy* (2026), <https://epic.org/issues/consumer-privacy/competition-and-privacy/>.

¹⁷ See e.g., Comments of EPIC, On the Consumer Financial Data Rights Rulemaking, CFPB (Jan. 25, 2023), <https://epic.org/wp-content/uploads/2023/01/EPIC-Comment-CFPB-Financial-Data-Rights-Rulemaking-Jan2023.pdf> (urging the CFPB to promulgate rules that protect privacy and empower consumers); Comments of EPIC, On the Prohibition on Creditors and Consumer Reporting Agencies Concerning Medical Information, CFPB, Docket No. CFPB-2024-0023 (Aug. 12, 2024), <https://epic.org/documents/comments-of-epic-to-the-cfpb-on-the-prohibition-on-creditors-and-consumer-reporting-agencies-concerning-medical-information/> (supporting the CFPB’s proposals to prohibit inclusion of medical debt on credit reports); Comments of EPIC, On the Small Business Advisory Review Panel for Consumer Reporting Rulemaking, CFPB (Oct. 30, 2023), <https://epic.org/documents/comments-of-epic-to-the-cfpb-on-the-small-business-advisory-review-panel-for-consumer-reporting-rulemaking/> (recommending refinements and additional provisions to the CFPB’s proposed revisions to Fair Credit Reporting Act rules which would clarify that data brokers must comply with the Act).

Any guidance should not dismiss privacy concerns when evaluating competition harm. Take the remedies brought forth in the DOJ’s *United States et al. v. Google* case where the court found that Google had an illegal monopoly over general search engine services and text advertising.¹⁸ In the remedies stage of the proceedings, the court barred the tech giant from entering or maintaining exclusive contracts related to the distribution of its products, ordered Google to share its data index with competitors, and ordered Google to offer search and search text ads syndication services to competitors.¹⁹ These remedies do not go far enough to meaningfully protect user privacy or restrict Google’s anticompetitive practices. Ordering Google to apply “appropriate privacy-enhancing techniques” to its data transferring with competitors without specifying the types of techniques that Google must use does not provide sufficient protections for its users’ personal information. Notably in January 2026, Google entered a multi-year partnership with Apple to use Google’s Gemini models and cloud computing services for Apple’s AI products—a move that appears structurally similar to what Google has done before for search-default arrangements but now with AI.²⁰ The Google case demonstrates that remedies that fail to sufficiently protect consumer privacy do not fix competition issues.

EPIC urges the FTC and DOJ to consider data privacy when developing guidance on collaboration among competitors because privacy encourages competition, innovation, and protects consumers. Privacy cannot be an afterthought and should be regarded as an essential part of competition. The Agencies have an opportunity to address emerging technology and modern business realities that the 2000 Guidelines did not consider such as algorithmic pricing harms

¹⁸ *United States v. Google LLC*, 747 F. Supp. 3d 1, 187 (D.D.C. 2024).

¹⁹ *United States v. Google LLC*, 803 F. Supp. 3d 18, 93 (D.D.C. 2025).

²⁰ Kalley Huang, *Apple Teams Up With Google for A.I. in Its Products*, N.Y. Times (Jan. 12, 2026), <https://www.nytimes.com/2026/01/12/technology/apple-google-ai-partnership.html>.

stemming from business mergers and joint ventures. Privacy, especially in the age of big data, plays a vital role in business collaboration and competition. Any guidance issued should reflect that. If you have any additional questions, please contact Enid Zhou at zhou@epic.org.

Sincerely,

/s/ Enid Zhou
Senior Counsel

/s/ Sara Geoghegan
Senior Counsel &
Director, Consumer Privacy Program

ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 New Hampshire Ave. NW
Washington, DC 20036
202-483-1140 (tel)
202-483-1248 (fax)