to try to identify which characteristics are sensitive and which are not. ''[T]he list of things that can trigger each unique individual's trauma is endless and would cover every imaginable'' advertisement based on every possible categorization, so whatever lines we end up drawing will be ''either arbitrary or highly politicized.'' [26]

We can already see this dysfunction in these complaints, which mention as sensitive characteristics race, ethnicity, gender, gender identity, sexual orientation, pregnancy, parenthood, health conditions, religion, and attendance of a political protest, among others.[27] While some of these characteristics often entail private facts, others are not usually considered private information. Attending a political protest, for example, is a public act. The public expression of dissatisfaction or support is the point of a protest. Treating attendance at a political protest as uniquely private and sensitive is an oxymoron. Moreover, there are no objective criteria on which to base this list.[28] The statute provides no guidance. The list is therefore a purely subjective creation of Commission bureaucrats. And it excludes categories that many would consider deeply private and sensitive.[29] And if we did a full accounting of characteristics that someone, somewhere might consider sensitive, no useful categorizations would remain. If what we are worried about is that the generation and sale of these categorizations will be a substitute for the sale of the user data from which they are derived, the correct approach is to treat conclusions derived from user data as no different than the underlying data. In either case, adequate consent is required for their collection, use, and sale.

Finally, I have doubts about the viability of a final charge levied against Mobilewalla for indefinitely retaining consumer location information.[30] It is a truism that data stored indefinitely is at a greater risk of compromise than data stored for a short period of time. But nothing in section 5 forms the basis of standards for data retention. The difficulty is illustrated perfectly by the proposed order we approve today. Rather than impose any particular retention schedule, it merely requires that Mobilewalla:

> . . . document, adhere to, and make publicly available . . . a retention schedule . . . setting forth: (1) the purpose or purposes for which each type of Covered Information is collected or used; (2) the specific business needs for retaining each type of Covered Information; and (3) an established timeframe for deletion of each type of Covered Information limited to the time reasonably necessary to fulfill the purpose for which the Covered Information was collected, and in no instance providing for the indefinite retention of any Covered Information . . .[31]

Given that Mobilewalla is in the business of selling user information, and that the marginal cost of data storage is low, the ''specific business need'' can be nothing more than the possible existence in the future of some buyer willing to pay more than the low cost of storage to acquire the data. I see no reason why Mobilewalla could not set a retention period of many decades based on this reasoning. In fact, while two-year-old location data is intuitively less valuable than one-year-old location data, it is quite plausible that twenty- or thirty-year-old location data is more valuable than location data that is only a few years old, as it may allow advertisers to tap into nostalgic sentiments.

The trouble with both the sensitive-categories count and the data-retention count is that the text of section 5 cannot bear the tremendous weight my colleagues place on it. My colleagues want the FTC Act to be a comprehensive privacy law. But it is not. Comprehensive privacy regulation involves difficult choices and expensive tradeoffs. Congress alone can make those choices and tradeoffs. It did not do so when it adopted the general prohibitions of section 5 nearly nine decades ago. And it has not adopted comprehensive privacy legislation since then. We must respect that choice.

Until Congress acts, we should vigorously protect Americans' privacy by enforcing the laws Congress has actually passed. But we must not stray from the bounds of the law. If we do, we will sow uncertainty among legitimate businesses, potentially disrupt the ongoing negotiations in Congress on privacy legislation, and risk damaging losses for the Commission in court.

[FR Doc. 2024–28738 Filed 12–5–24; 8:45 am]

BILLING CODE 6750–01–P

[26] Concurring and Dissenting Statement of Commissioner Andrew N. Ferguson, A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services, at 5 (Sept. 19, 2024), *https://www.ftc.gov/system/files/ftc_gov/pdf/ferguson-statement-social-media-6b.pdf.*

[27] Mobilewalla Complaint ¶¶ 27–32.

[28] See *Kyllo* v. *United States,* 533 U.S. 27, 38–39 (2001) (rejecting a Fourth Amendment rule that limited thermal-imaging data collection to only ''intimate details'' because of the impossibility of developing a principled distinction between intimate and nonintimate information).

[29] Gun ownership is an example. In many States, citizens are free to own guns without registering them. There is therefore no public record that a person owns a gun. And in constitutional-carry States, a citizen may carry his handgun in concealment without the government's permission, which means that bearing a firearm outside the home remains a private act. I expect many Americans would be horrified if their sensitive location data were used to place them in a ''gun owner'' category, and that category were then sold to other firms or to the government—particularly banks have gotten in the habit of ejecting customers who engaged in disfavored activities. Yet gun ownership does not make the Commission's list. But political protests do. It is hard to see this list as anything other than the product of arbitrary or political decision making.

[30] Mobilewalla Complaint ¶¶ 73–74.

[31] Decision and Order, *In re Mobilewalla, Inc.,* at 13.

FEDERAL TRADE COMMISSION

[File No. 202 3196]

Mobilewalla Inc.; Analysis of Proposed Consent Order To Aid Public Comment

AGENCY: Federal Trade Commission.

ACTION: Proposed consent agreement; request for comment.

SUMMARY: The consent agreement in this matter settles alleged violations of Federal law prohibiting unfair or deceptive acts or practices. The attached Analysis of Proposed Consent Order to Aid Public Comment describes both the allegations in the complaint and the terms of the consent order—embodied in the consent agreement—that would settle these allegations.

DATES: Comments must be received on or before January 6, 2025.

ADDRESSES: Interested parties may file comments online or on paper by following the instructions in the Request for Comment part of the **SUPPLEMENTARY INFORMATION** section below. Please write ''Mobilewalla; File No. 202 3196'' on your comment and file your comment online at *https://www.regulations.gov* by following the instructions on the web-based form. If you prefer to file your comment on paper, please mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Mail Stop H–144 (Annex D), Washington, DC 20580.

FOR FURTHER INFORMATION CONTACT: David Walko (202–326–2775), Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

SUPPLEMENTARY INFORMATION: Pursuant to section 6(f) of the Federal Trade Commission Act, 15 U.S.C. 46(f), and FTC Rule § 2.34, 16 CFR 2.34, notice is hereby given that the above-captioned consent agreement containing a consent order to cease and desist, having been

filed with and accepted, subject to final approval, by the Commission, has been placed on the public record for a period of 30 days. The following Analysis to Aid Public Comment describes the terms of the consent agreement and the allegations in the complaint. An electronic copy of the full text of the consent agreement package can be obtained at *https://www.ftc.gov/news-events/commission-actions.*

You can file a comment online or on paper. For the Commission to consider your comment, we must receive it on or before January 6, 2025. Write ''Mobilewalla; File No. 202 3196'' on your comment. Your comment—including your name and your State—will be placed on the public record of this proceeding, including, to the extent practicable, on the *https://www.regulations.gov* website.

Because of heightened security screening, postal mail addressed to the Commission will be subject to delay. We strongly encourage you to submit your comments online through the *https://www.regulations.gov* website. If you prefer to file your comment on paper, write ''Mobilewalla; File No. 202 3196'' on your comment and on the envelope, and mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Mail Stop H–144 (Annex D), Washington, DC 20580.

Because your comment will be placed on the publicly accessible website at *https://www.regulations.gov,* you are solely responsible for making sure your comment does not include any sensitive or confidential information. In particular, your comment should not include sensitive personal information, such as your or anyone else's Social Security number; date of birth; driver's license number or other State identification number, or foreign country equivalent; passport number; financial account number; or credit or debit card number. You are also solely responsible for making sure your comment does not include sensitive health information, such as medical records or other individually identifiable health information. In addition, your comment should not include any ''trade secret or any commercial or financial information which . . . is privileged or confidential''—as provided by section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule § 4.10(a)(2), 16 CFR 4.10(a)(2)—including competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

Comments containing material for which confidential treatment is requested must be filed in paper form, must be clearly labeled ''Confidential,'' and must comply with FTC Rule § 4.9(c). In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request and must identify the specific portions of the comment to be withheld from the public record. *See* FTC Rule § 4.9(c). Your comment will be kept confidential only if the General Counsel grants your request in accordance with the law and the public interest. Once your comment has been posted on the *https://www.regulations.gov* website—as legally required by FTC Rule § 4.9(b)—we cannot redact or remove your comment from that website, unless you submit a confidentiality request that meets the requirements for such treatment under FTC Rule § 4.9(c), and the General Counsel grants that request.

Visit the FTC website at *https://www.ftc.gov* to read this document and the news release describing the proposed settlement. The FTC Act and other laws the Commission administers permit the collection of public comments to consider and use in this proceeding, as appropriate. The Commission will consider all timely and responsive public comments it receives on or before January 6, 2025. For information on the Commission's privacy policy, including routine uses permitted by the Privacy Act, see *https://www.ftc.gov/site-information/privacy-policy.*

Analysis of Proposed Consent Order To Aid Public Comment

The Federal Trade Commission (''Commission'') has accepted, subject to final approval, an agreement containing a consent order from Mobilewalla Inc. (''Mobilewalla''). The proposed consent order (''Proposed Order'') has been placed on the public record for 30 days for receipt of public comments from interested persons. Comments received during this period will become part of the public record. After 30 days, the Commission will again review the agreement, along with the comments received, and will decide whether it should make final the Proposed Order or withdraw from the agreement and take appropriate action.

Respondent Mobilewalla is a Delaware company with its headquarters in Georgia. Founded in 2008, Mobilewalla is a data broker that aggregates consumer information, including location data, to use and sell for its clients' purposes, including marketing, analytics, and non-commercial uses.

Mobilewalla does not collect information directly from consumers. Instead, Mobilewalla purchases consumers' location data and other personal information, including consumers' unhashed and hashed phone numbers from third-party data brokers. Mobilewalla has also collected data through real-time bidding (''RTB'') exchanges and other advertising platforms.

When Mobilewalla bid to place an advertisement for its clients through an RTB exchange, Mobilewalla collected and retained the information contained in the bid request, including the device's mobile advertising identifier (''MAID''), a timestamp, and precise location data, if the consumer had location sharing turned on.

Mobilewalla has sold or licensed raw consumer data, including a device's latitude and longitude coordinates paired with MAIDs, to its clients. Mobilewalla also analyzes the location data it obtains and, based on the locations and events visited by consumers' mobile devices, categorizes MAIDs into ''audience segments'' based on interests or characteristics purportedly revealed by the locations or events. Mobilewalla has offered standard audience segments such as ''Music Lovers'' but has also created custom audience segments for clients, such as audience segments targeting pregnant women, Hispanic churchgoers, and members of the LGBTQ+ community.

Mobilewalla does not take sufficient steps to verify that consumers consent to its use of their data. Mobilewalla relies on its data suppliers to obtain consumer consent for the collection and use of their data. Mobilewalla's contracts with its data suppliers include vague provisions requiring the suppliers to comply with applicable law when transferring consumer data to Mobilewalla but does not specifically require consumer consent. In addition, Mobilewalla has minimal procedures to verify whether its suppliers obtained consumer consent. Mobilewalla typically evaluates new data suppliers through a questionnaire and by reviewing the disclosures to consumers from three to five apps from which the supplier collects consumers' data, even though some suppliers collect consumers' data from thousands of apps. Mobilewalla does not subsequently or periodically check whether the apps have changed their disclosures.

In addition to failing to take sufficient steps to verify consumer consent,

Mobilewalla has retained the collected data indefinitely—far longer than necessary to accomplish the purpose of collection. This unreasonable retention period, combined with Mobilewalla's comprehensive data collection practices, significantly increases the risk that the sensitive location data would be disclosed or misused, causing harm to consumers.

The Commission's proposed five-count complaint alleges that Mobilewalla violated section 5(a) of the FTC Act by (1) unfairly selling consumers' sensitive location information, (2) unfairly targeting consumers based on sensitive characteristics, (3) unfairly collecting consumers' information from RTB exchanges, (4) unfairly collecting and using consumer location information without consent verification, and (5) unfairly retaining consumer location information.

With respect to the first count, the proposed complaint alleges that Mobilewalla sold consumers sensitive location information associated with unique persistent identifiers that reveal consumers' visits to sensitive locations. With respect to the second count, the proposed complaint alleges Mobilewalla has categorized consumers into audience segments based on sensitive characteristics, such as medical conditions and religious beliefs, derived from location data. Mobilewalla has sold or transferred these audience segments to third parties for marketing and other purposes, including identifying and targeting consumers who participate in political rallies and protests or attempting to identify and target consumers who participate in union organizing.

With respect to the third count, the proposed complaint alleges that Mobilewalla collected consumers' personal information, including location data, from RTB exchanges, when Mobilewalla had no winning bid. With respect to the fourth count, the proposed complaint alleges that Mobilewalla failed to take reasonable steps to verify that consumers consent to Mobilewalla's use of their location data to track them, develop audience segments, target them with advertising, and use and share their location information with clients for commercial, political, law enforcement, and other purposes. Despite collecting data from thousands of apps, Mobilewalla only checked a very small number of apps to determine whether the app disclosed that the app collected location information and shared it with third parties. Mobilewalla also did not periodically check apps' disclosures, even though many apps change their disclosures over time.

With respect to the fifth count, the proposed complaint alleges that Mobilewalla retained detailed, sensitive information about consumers, including their location data, indefinitely, which is longer than reasonably necessary to fulfill the purpose for which that information was collected. This practice caused substantial injury in the form of a loss of privacy about the day-to-day movements of millions of consumers, including through the use of retroactive geofences, and an increased risk of disclosure and use of such sensitive information.

The proposed complaint alleges that Mobilewalla has caused or is likely to cause substantial injury in the form of loss of privacy about day-to-day movements of consumers and an increased risk of disclosure of such sensitive information. Additionally, with respect to the fourth count, the proposed complaint alleges that Mobilewalla has caused or is likely to cause substantial injury in the form of the chilling of consumers' First Amendment rights and an increased risk of public or harmful disclosure of sensitive information about consumers' private lives, including their fertility choices, religious worship, sexuality, and other such sensitive information.

Summary of Proposed Order With Respondent

The Proposed Order contains injunctive relief designed to prevent Mobilewalla from engaging in the same or similar acts or practices in the future. Geolocation data can vary significantly in its precision. The privacy concerns posed by the proposed complaint relate to more precise location data—that is, location data that could be used to identify specific locations a consumer visits. As a result, the Proposed Order is limited to location data that identifies consumers' locations in a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet.

Provision I prohibits Mobilewalla from misrepresenting (1) the extent to which it collects, maintains, uses, discloses, or deletes location data, and (2) the extent to which such data is deidentified. Provision II prohibits Mobilewalla from collecting or retaining consumer information that Mobilewalla accesses while participating in RTB exchanges for any other purpose than participating in the auctions that occur on the exchange.

Provision III prohibits Mobilewalla from selling, licensing, transferring, sharing, disclosing, or using sensitive location data in any products or services.

Sensitive locations are defined as those locations associated with (1) medical facilities (*e.g.,* family planning centers, general medical and surgical hospitals, offices of physicians, offices of mental health physicians and practitioners, residential mental health and substance abuse facilities, outpatient mental health and substance abuse centers, outpatient care centers, psychiatric and substance abuse hospitals, and specialty hospitals); (2) religious organizations;(3) correctional facilities; (4) labor union offices; (5) locations held out to the public as predominantly providing education or childcare services to minors; (6) locations held out to the public as predominantly providing services to LGBTQ+ individuals such as service organizations, bars and nightlife; (7) locations held out to the public as predominantly providing services based on racial or ethnic origin; or (8) locations held out to the public as predominantly providing temporary shelter or social services to homeless, survivors of domestic violence, refugees, or immigrants; (9) locations of public gatherings of individuals during political or social demonstrations, marches, and protests; or (10) military installations, offices, or buildings.

Provision IV requires that Mobilewalla implement and maintain a sensitive location data program to develop a comprehensive list of sensitive locations and to prevent the use, sale, license, transfer, or disclosure of sensitive location data. Provision V prohibits Mobilewalla from selling or disclosing Location Data that may determine the identity or location of an individual's private residence.

Provision VI requires Mobilewalla to implement a Supplier Assessment Program by which they assess their suppliers and help ensure that consumers have provided consent for the collection and use of Location Data obtained by Mobilewalla. Under this program, Mobilewalla must conduct initial assessments of all suppliers within 30 days of entering into a data sharing agreement. The program also requires that Mobilewalla confirm that consumers provide Affirmative Express Consent, if feasible, or confirm that consumers provide specific consent to the collection, use, and sale of their location data. Mobilewalla must also create and maintain records of its Suppliers' assessment responses. Finally, Mobilewalla must cease from using, selling, or disclosing location data for which consumers do not provide consent.

Provision VII requires Mobilewalla to provide a clear and conspicuous means for consumers to request the identities of any third parties to whom Respondent sold or otherwise disclosed their location data during the one-year period preceding the request. Provision VIII requires Mobilewalla to provide a simple, easily-located means for consumers to withdraw any consent provided and Provision IX requires Mobilewalla to delete and cease collecting location data after Mobilewalla receives notice that the consumer has withdrawn their consent. Provision X also requires Mobilewalla to provide a simple, easily-located means for consumers to request that Mobilewalla delete location data that Mobilewalla previously collected and to delete the location data within 30 days of receipt of such request.

Provision XI requires that Mobilewalla (1) document and adhere to a retention schedule for the covered information it collects from consumers, including the purposes for which it collects such information, the specific business needs, and an established timeframe for its deletion, and (2) prior to collecting or using new type of information related to consumers that was not previously collected, and is not described in its retention schedule, update its retention schedule. Provision XII requires Mobilewalla to delete any historic location data and consumers' unhashed and hashed phone numbers in their control and any work product created from this data and to instruct their customers to also delete this information, unless Mobilewalla contains a record in accordance with the Supplier Assessment Program (Provision VI) that consumers consented to the collection, use, and disclosure of their historic location data or the historic location data is deidentified or rendered non-sensitive. Provision XIII requires Mobilewalla to establish and implement, and thereafter maintain, a comprehensive privacy program that protects the privacy of consumers' personal information.

Provisions XIV–XVII are reporting and compliance provisions, which include recordkeeping requirements and provisions requiring Mobilewalla to provide information or documents necessary for the Commission to monitor compliance. Provision XVIII states that the Proposed Order will remain in effect for 20 years, with certain exceptions.

The purpose of this analysis is to facilitate public comment on the Proposed Order, and it is not intended to constitute an official interpretation of the complaint or Proposed Order, or to modify the Proposed Order's terms in any way.

By direction of the Commission, Commissioner Holyoak dissenting.

April J. Tabor,

Secretary.

Statement of Chair Lina M. Khan Joined by Commissioner Alvaro M. Bedoya

Last year a new report revealed the relative ease with which foreign adversaries can gather sensitive data on Americans.[1] Foreign states could identify, for example, whether someone has a substance abuse problem, a gambling addiction, or major financial problems—a ''torrent of blackmail data'' ripe for abuse.[2] The report noted that people susceptible to this type of surveillance include active military personnel, defense officials, lawmakers, and judges. Beyond government employees, hundreds of millions of Americans are at risk. Precise location data, for example, can be harnessed by managers tracking employees suspected of workplace organizing, law enforcers monitoring protestors who oppose government policies, or stalkers keeping tabs on their victims.

The mechanism for this surveillance is shockingly commonplace: ''real-time bidding'' (RTB) exchanges, an advertising technology present on a huge swath of websites and apps. RTB exchanges host the online auctions that determine which advertisement gets served to a specific individual on a specific website or app. Because these ads are targeted, RTB technology captures reams of personal data, such as a person's browsing history and their location and movements over time—and then broadcasts this sensitive data to anyone seeking to bid on the ad slot. One report estimates that RTB technologies track and broadcast what every U.S. internet user does every 30 seconds they are online—or 747 times a day on average.[3] Strikingly, a firm can capture and retain individuals' web browsing data, location data, and other sensitive details even when it does not serve any ads to them. As lawmakers have noted, the exposure of this bidstream data creates an ''outrageous privacy violation'' [4] as well as a major threat to national security.[5]

Today the FTC is bringing an enforcement action against surveillance practices that illegally harness RTB data—the first time the Commission has taken action against the use of this ''bidstream'' data. Specifically, our action against Mobilewalla charges that the data broker, among other things, unfairly collected people's sensitive data (including precise location) from real-time bidding exchanges—even when it did not place an ad through the bid.

This conduct was part of a broader set of practices that Mobilewalla undertook to unlawfully collect, sell, and retain sensitive information on millions of Americans. Our investigation uncovered that Mobilewalla gathered large swaths of people's personal information, including location data, and sold ''audience segments'' that third parties could use to target people based on sensitive characteristics. Mobilewalla's audience segments included, for example, Hispanic churchgoers, pregnant women, members of the LGBTQ+ community, workers participating in union organizing, and people who participate in political rallies. Mobilewalla built these profiles through a variety of mechanisms beyond its use of bidstream data, such as by creating ''geo-fences'' around places like pregnancy centers, political protests, and state capitols.[6] Mobilewalla even began collecting people's phone numbers, which, paired with MAIDs, could be used to identify the person frequenting a specific location.

The Commission's complaint charges that Mobilewalla's practices constituted unfair conduct in violation of the FTC Act. Specifically, the complaint alleges that: (1) Mobilewalla's sale of people's sensitive location data is unfair; (2) Mobilewalla's sale and transfer of audience segments based on sensitive characteristics—like their medical conditions, religious beliefs,

[1] Irish Council for Civil Liberties, America's Hidden Security Crisis: How Data About United States Defence Personnel & Political Leaders Flows to Foreign States & Non-State Actors (2023), *https://www.iccl.ie/wp-content/uploads/2023/11/Americas-hidden-security-crisis.pdf. See also* Justin Sherman, et al., *Data Brokers and the Sale of Data on U.S. Military Personnel Risks to Privacy, Safety, and National Security* (Duke Univ. Sanford Sch. of Pub. Pol'y 2023), *https://techpolicy.sanford.duke.edu/data-brokers-and-the-sale-of-data-on-us-military-personnel/;* Joseph Cox, *The Hundreds of Little-Known Firms Getting Data on Americans, Vice* (June 28, 2021), *https://www.vice.com/en/article/hundreds-companies-bidstream-data-location-browsing/.*

[2] *Id.*

[3] *Id.* at p. 7.

[4] Letter from Sen. Wyden to Chair Simons (July 30, 2020), *https://www.wyden.senate.gov/imo/media/doc/073120_Wyden_Cassidy_Led_FTC_Investigation_letter.pdf.*

[5] Joseph Cox, *Congress Says Foreign Intel Services Could Abuse Ad Networks for Spying,* **VICE** (Apr. 6, 2021), *https://www.vice.com/en/article/congress-foreign-intelligence-agencies-bidstream-real-time-bidding/.*

[6] In one instance, one of Mobilewalla's clients used its data to ''geo-fence the homes of individuals relevant to a private lawsuit and track where those individuals had traveled to over the preceding two years, including whether they visited federal law enforcement offices.'' Complaint, *In re Mobilewalla, Inc.,* FTC File No. 2023196 (Dec. 3, 2024) at ¶ 50.

participation in workplace organizing, or attendance at political protests—is unfair; (3) Mobilewalla's collection of people's personal information, including geolocation data, from RTB exchanges even when Mobilewalla had no winning bid is unfair; (4) Mobilewalla's failure to take reasonable steps to verify that users consent to its use of their location data to surveil them, develop audience segments based on sensitive characteristics, target them with advertising, and disseminate their location data with a host of clients is unfair, and (5) Mobilewalla's indefinite retention of people's sensitive location information is unfair.

The Commission's action against Mobilewalla marks the FTC's fifth case involving the illegal dissemination of geolocation information—all pursued in the last 28 months.[7] This steady clip of cases reflects our recognition that location data is among the most sensitive of people's data, revealing everything from where someone spends the night to what medical services they seek. Indeed, the District of Idaho last year recognized that invasions of privacy can substantially injure Americans, even without a showing of further harm.[8] And noting that ''location records hold for many Americans the 'privacies of life,' '' the Supreme Court has held that constitutional safeguards against unchecked government surveillance extend to digital location tracking—even when the data is originally collected by private companies.[9]

Today's action highlights two areas meriting continued focus for the Commission and policymakers concerned about threats to Americans' privacy. First, the ease with which real-time bidding technology can be exploited to surveil Americans should raise serious alarm. No real safeguards limit who can access, harness, or retain this data, meaning that the multi-billion-dollar industry built around targeted advertising leaves Americans' sensitive data shockingly exposed.

Second, this matter further highlights the continued shortcomings of the ''notice and consent'' paradigm. Most people never interact with Mobilewalla and have no idea that Mobilewalla amasses data detailing their precise location and movements. In theory, Mobilewalla would rely on its data suppliers to obtain consumer consent for the collection and use of their data. But in practice, Mobilewalla has minimal procedures to verify whether its suppliers actually obtained consumer consent—and many disclosures are broad enough to render consent effectively meaningless. In recent years, the Commission's orders have moved away from remedies and relief premised exclusively on consumer consent—and included greater reliance on presumptive bans and prohibitions.[10] Continuing to ensure our orders reflect the realities of how people engage in today's economy will be critical for Americans to enjoy real privacy.

I am grateful to the DPIP team for their excellent work on this matter.

[7] Press Release, Fed. Trade Comm'n, FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations (Aug. 29, 2022), *https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other;* Press Release, Fed. Trade Comm'n, FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data (Jan. 9, 2024), *https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data;* Press Release, Fed. Trade Comm'n, FTC Order Will Ban InMarket from Selling Precise Consumer Location Data (Jan. 18, 2024), *https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-will-ban-inmarket-selling-precise-consumer-location-data;* Press Release, Fed. Trade Comm'n, Gravy Analytics (Dec. 3, 2024), *https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-takes-action-against-gravy-analytics-venntel-unlawfully-selling-location-data-tracking-consumers.*

[8] Memorandum Decision & Order, *FTC* v. *Kochava Inc.,* 2:22–cv–00377–BLW (D. Idaho May 4, 2023) (''Thus, under the plain language of the FTC Act, a defendant whose acts or practices violate consumer privacy may be said to inflict an 'injury' upon consumers within the meaning of Section 5(n)'').

[9] *Carpenter* v. *United States,* 585 U.S. 296, 138 S. Ct. 2206, 2217 (2018) (quoting *Riley* v. *California,* 573 U.S. 373, 403 (2014)). *See also* Statement of Chair Lina M. Khan Joined by Comm'r Rebecca Kelly Slaughter and Comm'r Alvaro Bedoya In the Matter of X-Mode Social, Inc. and Outlogic, LLC (Jan. 9, 2024), *https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/statement-chair-lina-m-khan-joined-commissioner-rebecca-kelly-slaughter-commissioner-alvaro-bedoya-0;* Statement of Comm'r Alvaro Bedoya Joined By Chair Lina M. Khan In the Matter of Gravy Analytics (Dec. 3, 2024), *https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/statement-commissioner-alvaro-m-bedoya-joined-chair-lina-m-khan-commissioner-rebecca-kelly-slaughter-3.*

[10] *See, e.g.,* X-Mode, InMarket, *supra* note 7; Press Release, Fed. Trade Comm'n, FTC Order Will Ban Avast from Selling Browsing Data for Advertising Purposes, Require It to Pay $16.5 Million Over Charges the Firm Sold Browsing Data After Claiming Its Products Would Block Online Tracking (Feb. 22, 2024), *https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-order-will-ban-avast-selling-browsing-data-advertising-purposes-require-it-pay-165-million-over;* Press Release, Fed. Trade Comm'n, FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising (Feb. 1, 2023), *https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising.*

Concurring and Dissenting Statement of Commissioner Andrew N. Ferguson

Today the Commission approves complaints against, and proposed consent orders with, Gravy Analytics [1] (''Gravy'') [2] and Mobilewalla [3] for various practices concerning the collection and dissemination of precise location data allegedly constituting unfair or deceptive acts or practices in violation of section 5 of the Federal Trade Commission Act.[4] Gravy and Mobilewalla are data brokers that aggregate and sell consumer data, including location data.[5] Gravy and Mobilewalla do not collect the data from consumers.[6] Those data are collected from applications that consumers use on their smartphones, and Gravy and Mobilewalla purchase or otherwise acquire those data after they are collected.[7] Gravy and Mobilewalla then sell those data to private firms for advertising, analytics, and other purposes, as well as to the government.[8]

Part I

I concur entirely in two of the counts the Commission brings against both firms, and one that we bring against Mobilewalla alone. These counts are sufficient to justify my vote in favor of submitting the complaints and proposed consent orders for public comment. First, the Commission alleges that Gravy and Mobilewalla sell consumers' precise location data without taking sufficient measures to anonymize the information or filter out sensitive locations.[9] This type of data—records of a person's precise physical locations—is inherently intrusive and revealing of people's most private affairs. The sale of such revealing information that can be linked directly to an individual consumer poses an obvious risk of

[1] Also named is Venntel, Inc., a wholly-owned subsidiary of Gravy Analytics.

[2] Complaint, *In re Gravy Analytics* (''Gravy Complaint'').

[3] Complaint, *In re Mobilewalla* (''Mobilewalla Complaint'').

[4] 15 U.S.C. 45.

[5] Gravy Complaint ¶ 7; Mobilewalla Complaint ¶¶ 3, 18.

[6] Gravy Complaint ¶ 8; Mobilewalla Complaint ¶ 4.

[7] Gravy Complaint ¶¶ 9–10; Mobilewalla Complaint ¶¶ 4, 5.

[8] Gravy Complaint ¶¶ 13–21; Mobilewalla Complaint ¶¶ 6, 19, 36. As my colleagues' statements make clear, the sale of data to the government for law-enforcement, national-security, and immigration-enforcement purposes implicates different constitutional and statutory questions than the sale of those same data to private firms. I take no firm position on those questions except to say that I believe that the restrictions on sale to the government in the Gravy order are lawful.

[9] Gravy Complaint ¶¶ 73–75; Mobilewalla Complaint ¶¶ 66–67.

substantial injury to that consumer.[10] The theft or accidental dissemination of those data would be catastrophic to the consumer. The consumer cannot avoid the injury. Unless the consumer has consented to the sale of intimate data linked directly to him, the sale of the data happens entirely without his knowledge.[11] Finally, given that the anonymized data remain valuable to firms for advertising and analytics, the injury that the consumer suffers is not outweighed by any countervailing benefits for the consumer.[12] The sale of non-anonymized, precise location data without first obtaining the meaningfully informed consent of the consumer is therefore an unfair act or practice in violation of section 5.

Second, the Commission accuses both companies of collecting, using, and selling precise location information without sufficiently verifying that the consumers who generated the data consented to the collection of those data by the applications that collected it.[13] Given that the failure to obtain meaningful consent to the collection of precise location data is widespread, data brokers that purchase sensitive information cannot avoid liability by turning a blind eye to the strong possibility that consumers did not consent to its collection and sale. The sale of precise location data collected without the consumer's consent poses a similarly unavoidable and substantial risk of injury to the consumer as does the sale of the non-anonymized data. I therefore concur in these counts against Gravy and Mobilewalla.[14]

I further concur in one additional count charged against Mobilewalla alone. The Commission accuses it of having committed an unfair act or practice for its conduct on real-time bidding exchanges (RTBs).[15] An RTB is a marketplace where advertisers bid in real time on the opportunity to show an advertisement to a user as the user is visiting a website or using an application.[16] The auctions take place in the blink of an eye, and the listings on which advertisers bid include information such as the user's mobile advertising ID (MAIDs) and current precise location.[17] Advertisers crave these data because it allows them to maximize the value of each ad impression by displaying the ads only to the users most likely to find the advertisement useful. The Commission accuses Mobilewalla of sitting on the RTBs, submitting bids, collecting the MAIDs and location data for the bids, retaining those data even when it did not win the auction, and combining those data with data acquired from other sources to identify the user represented by the MAID.[18] It aggregated and sold this combined identity and location information to its clients.[19] This alleged practice violated Mobilewalla's legal contracts with the exchanges.[20]

The violation of a private contract alone is not enough to establish a violation of section 5.[21] But these agreements protected more than just Mobilewalla's contractual counterparties. They also protected large numbers of consumers from the risk of having their private data aggregated, linked to their identity, and sold without their consent, as Mobilewalla did. Mobilewalla's breach of its contractual obligations therefore exposed consumers to the same substantial risk of injury as collection of their data without consent, was not reasonably avoidable by consumers (as this conduct was far removed from their knowledge and control), and was not outweighed by any countervailing benefits to consumers. It is therefore in the public interest to hold Mobilewalla liable for this conduct under section 5, as it would be even if no contract governed Mobilewalla's obligations regarding the unconsented collection and retention of these precise location data.[22]

Part II

I dissent from the Commission's counts against both firms accusing them of unfairly categorizing consumers based on sensitive characteristics, and of selling those categorizations to third parties.[23] The FTC Act prohibits the collection and subsequent sale of precise location data for which the consumer has not consented to the collection or sale. It further requires data brokers to take reasonable steps to ensure that consumers originally consented to the collection of the data that the data brokers subsequently use and sell. If a company aggregates and categorizes data that were collected without the consumer's consent, and subsequently sells those categorizations, it violates section 5. But it does so only because the data were collected without consent for such use, not because the categories into which it divided the data might be on an indeterminate naughty categories list. The FTC Act imposes consent requirements in certain circumstances. It does not limit how someone who lawfully acquired those data might choose to analyze those data, or the conclusions that one might draw from them.[24]

Consider an analogous context: the collection of data by private investigators. Private investigators do not violate the law if they follow someone on the public streets to his place of employment, observe him entering a church, observe him attending the meeting of a political party, or watch him enter a hospital. These are all public acts that people carry out in the sight of their fellow citizens every day. Nor do private investigators violate the law by concluding from their lawful observations that the person works for that company, practices that religion, belongs to that political party, or suffers from an illness. Nor would the law prohibit the private investigator from selling his conclusions to a client. But the law would forbid private investigators from trespassing on the employer's property; from surreptitiously planting cameras inside

[10] 15 U.S.C. 45(n); see *FTC* v. *Kochava, Inc.,* 715 F. Supp. 3d 1319, 1323–24 (D. Idaho 2024).

[11] 15 U.S.C. 45(n).

[12] *Ibid.*

[13] Gravy Complaint ¶¶ 76–78; Mobilewalla Complaint ¶¶ 71–72.

[14] Section 5 does not impose strict liability for the purchase of precise location data collected without the consumer's consent, nor do I understand the complaints and orders as interpreting section 5 hold data brokers strictly liable for every purchase of precise location data that was collected without the consumer's consent. Data brokers need only take reasonable steps to ensure that the data they are acquiring were originally collected with the consumer's consent. Gravy Complaint ¶ 76 (faulting Gravy for not taking ''reasonable steps to verify that consumers provide informed consent to Respondents' collection, use, or sale of the data for commercial and government purposes.''); Mobilewalla Complaint ¶ 71 (similar).

[15] Mobilewalla Complaint ¶ 70.

[16] *Id.* ¶ 9.

[17] *Ibid.*

[18] *Id.* ¶¶ 12–15.

[19] *Id.* ¶ 18.

[20] Mobilewalla Complaint ¶ 10.

[21] See *FTC* v. *Klesner,* 280 U.S. 19, 28 (1929) (Section 5's requirement that enforcement ''would be to the interest of the public'' is not satisfied in the case of a purely private dispute, as ''the mere fact that it is to the interest of the community that private rights shall be respected is not enough to support a finding of public interest.'').

[22] See *id.* at 27–28 (explaining that protection of private rights can be incident to the public interest, and that such cases might include those where the conduct threatens the existence of competition, involves the ''flagrant oppression of the weak by the strong,'' or where the aggregate loss is sufficient to make the matter one of public consequence but incapable of vindication by individual private suits).

[23] Gravy Complaint ¶¶ 79–81; Mobilewalla Complaint ¶¶ 68–69.

[24] Of course, other laws might prohibit particular uses of data that were collected consistently with the requirements of section 5. Using lawfully obtained data to draw conclusions about a consumer's race alone would not violate section 5, but using those conclusions to make an employment or housing decision, for example, might violate the Civil Rights Act of 1964, 42 U.S.C. 2000e *et seq.,* or the Fair Housing Act, 42 U.S.C. 3601 *et seq.* But merely drawing a conclusion from lawfully obtained data does not violate section 5.

the church sanctuary to observe the rites; from recording the proceedings of the political meeting without consent; or from extorting hospital staff for information about the person's condition. The law prohibits collecting data in unlawful ways; it does not prohibit drawing whatever conclusions one wants, or selling those conclusions to someone else, so long as the data from which the conclusions were drawn were lawfully obtained.

The same principle should apply to section 5. The added wrinkle is that in the information economy, private data are usually collected in the context of a commercial relationship between the user and the developer of an application or website. Just as we expect a merchant to disclose the material terms of a transaction before collecting payment, we expect that the user of an app or website be informed of how their private information—part, and often all, of the consideration they give in exchange for use of the app or website—will be collected and used, and given a chance to decline the transaction. Commercial fairness might also require more than vague hidden disclosures, especially when the loss of privacy is substantial, as is the case with collection of precise location data and its sale to third parties.

Rather than faulting these companies for disclosing data about users without adequate consent, these counts in the complaints focus instead on the inherent impropriety of categorizing users according to so-called ''sensitive characteristics.'' Perhaps my colleagues are worried that advertisements targeted on the basis of these categories can cause emotional distress—the theory they advanced in the Commission's Social Media 6(b) Report earlier this year.[25] But as I argued then, it is folly to try to identify which characteristics are sensitive and which are not. ''[T]he list of things that can trigger each unique individual's trauma is endless and would cover every imaginable'' advertisement based on every possible categorization, so whatever lines we end up drawing will be ''either arbitrary or highly politicized.'' [26]

We can already see this dysfunction in these complaints, which mention as sensitive characteristics race, ethnicity, gender, gender identity, sexual orientation, pregnancy, parenthood, health conditions, religion, and attendance of a political protest, among others.[27] While some of these characteristics often entail private facts, others are not usually considered private information. Attending a political protest, for example, is a public act. The public expression of dissatisfaction or support is the point of a protest. Treating attendance at a political protest as uniquely private and sensitive is an oxymoron. Moreover, there are no objective criteria on which to base this list.[28] The statute provides no guidance. The list is therefore a purely subjective creation of Commission bureaucrats. And it excludes categories that many would consider deeply private and sensitive.[29] And if we did a full accounting of characteristics that someone, somewhere might consider sensitive, no useful categorizations would remain. If what we are worried about is that the generation and sale of these categorizations will be a substitute for the sale of the user data from which they are derived, the correct approach is to treat conclusions derived from user data as no different than the underlying data. In either case, adequate consent is required for their collection, use, and sale.

Finally, I have doubts about the viability of a final charge levied against Mobilewalla for indefinitely retaining consumer location information.[30] It is a truism that data stored indefinitely is at a greater risk of compromise than data stored for a short period of time. But nothing in section 5 forms the basis of standards for data retention. The difficulty is illustrated perfectly by the proposed order we approve today. Rather than impose any particular retention schedule, it merely requires that Mobilewalla:

> . . . document, adhere to, and make publicly available . . . a retention schedule . . . setting forth: (1) the purpose or purposes for which each type of Covered Information is collected or used; (2) the specific business needs for retaining each type of Covered Information; and (3) an established timeframe for deletion of each type of Covered Information limited to the time reasonably necessary to fulfill the purpose for which the Covered Information was collected, and in no instance providing for the indefinite retention of any Covered Information . . .[31]

Given that Mobilewalla is in the business of selling user information, and that the marginal cost of data storage is low, the ''specific business need'' can be nothing more than the possible existence in the future of some buyer willing to pay more than the low cost of storage to acquire the data. I see no reason why Mobilewalla could not set a retention period of many decades based on this reasoning. In fact, while two-year-old location data is intuitively less valuable than one-year-old location data, it is quite plausible that twenty- or thirty-year-old location data is more valuable than location data that is only a few years old, as it may allow advertisers to tap into nostalgic sentiments.

The trouble with both the sensitive-categories count and the data-retention count is that the text of section 5 cannot bear the tremendous weight my colleagues place on it. My colleagues want the FTC Act to be a comprehensive privacy law. But it is not. Comprehensive privacy regulation involves difficult choices and expensive tradeoffs. Congress alone can make those choices and tradeoffs. It did not do so when it adopted the general prohibitions of section 5 nearly nine decades ago. And it has not adopted comprehensive privacy legislation since then. We must respect that choice.

Until Congress acts, we should vigorously protect Americans' privacy by enforcing the laws Congress has actually passed. But we must not stray from the bounds of the law. If we do, we will sow uncertainty among legitimate businesses, potentially disrupt the ongoing negotiations in Congress on privacy legislation, and risk damaging losses for the Commission in court.

Dissenting Statement of Commissioner Melissa Holyoak

Since arriving at the Commission, I have supported law enforcement actions against data brokers that sold precise

[25] FTC, A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services, An FTC Staff Report, at 44 (Sept. 2024), *https://www.ftc.gov/system/files/ftc_gov/pdf/Social-Media-6b-Report-9-11-2024.pdf.*

[26] Concurring and Dissenting Statement of Commissioner Andrew N. Ferguson, A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services, at 5 (Sept. 19, 2024), *https://www.ftc.gov/system/files/ftc_gov/pdf/ferguson-statement-social-media-6b.pdf.*

[27] Mobilewalla Complaint ¶¶ 27–32.

[28] See *Kyllo* v. *United States,* 533 U.S. 27, 38–39 (2001) (rejecting a Fourth Amendment rule that limited thermal-imaging data collection to only ''intimate details'' because of the impossibility of developing a principled distinction between intimate and nonimtimate information).

[29] Gun ownership is an example. In many States, citizens are free to own guns without registering them. There is therefore no public record that a person owns a gun. And in constitutional-carry States, a citizen may carry his handgun in concealment without the government's permission, which means that bearing a firearm outside the home remains a private act. I expect many Americans would be horrified if their sensitive location data were used to place them in a ''gun owner'' category, and that category were then sold to other firms or to the government—particularly banks have gotten in the habit of ejecting customers who engaged in disfavored activities. Yet gun ownership does not make the Commission's list. But political protests do. It is hard to see this list as anything other than the product of arbitrary or political decision making.

[30] Mobilewalla Complaint ¶¶ 73–74.

[31] Decision and Order, *In re Mobilewalla, Inc.,* at 13.

geolocation data revealing consumers' religious beliefs, political leanings, and medical conditions.[1] Such enforcement actions have been particularly important where they help preserve Americans' freedoms and are consistent with the FTC Act, such as in a separate case the Commission brings against Gravy Analytics today. But the instant complaint and proposed settlement with Mobilewalla colors well outside the lines of the Commission's authority. Indeed, the Chair is seeking to effectuate legislative and policy goals that rest on novel legal theories well beyond what Congress has authorized. We should not use our enforcement powers this way.[2] Because core aspects of this case are misguided, I dissent. I briefly explain some of my concerns below. And I anticipate and welcome robust comment on the proposed order before it is finalized.

Several background considerations also inform my approach and dissent in this particular matter. First, this matter uses a settlement to effectuate policy objectives that political leadership at the Commission has sought for years but failed to achieve through regulation.[3] No matter how much political pressure Chair Khan and the Bureau Director may feel with the shot-clock running out, the Commission should not use complaints and orders to score political points that stem from misuse of our statutory authorities. Second and related: Chair Khan's decision to proceed runs directly afoul of recent Congressional oversight from several of the FTC's authorizing Committees that explicitly cautioned against this type of endeavor.[4] Choosing to proceed undermines our institutional legitimacy and will engender even more distrust from Congress—trust that current leadership at the Commission has repeatedly broken.[5]

With that larger context in mind, I will briefly describe some of my concerns on the merits. According to the Complaint, Mobilewalla has relied primarily on information it collected from real-time bidding exchanges (RTB exchanges) to build its portfolio of consumers' geolocation data.[6] These exchanges facilitate advertisers' bids to place content in front of specific consumers, whose information has been sent to the exchange to enable the bidding.[7] Mobilewalla would retain information collected from RTB exchanges, including a consumer's ''precise geolocation information, if the consumer had location sharing turned on,'' even if the bid were unsuccessful.[8]

The Majority erroneously declares Mobilewalla's collection of consumer information from the RTB exchanges is unfair. Specifically, the Complaint alleges that the practice of collecting data was unfair in part because it caused or is likely to cause substantial injury.[9] But the Complaint's allegations are remarkably sparse when it comes to establishing how the collection itself caused substantial injury, and its related allegations do not otherwise satisfy what section 5 requires for unfairness.[10] For the Majority, the mere collection of data implausibly ''causes or is likely to cause'' substantial injury and lacks countervailing benefits that section 5's cost-benefit analysis requires assessing.[11] Such a theory of unfairness—assertions about a particular practice without facts alleged reflecting causation of injury to consumers—is contrary to black-letter unfairness law. Of course, none of these observations about the limits of our unfairness authority mean Mobilewalla had clean hands under contract law, where Mobilewalla's agreements with RTB exchanges barred collection and retention of consumer data for unsuccessful bids.[12] But—contrary to what those keeping score may conclude from this case and settlement—a business-to-business breach of contract that may have potential effects on consumers does not automatically give rise to an unfairness claim under section 5.[13]

Count II, for ''Unfair Targeting Based on Sensitive Characteristics,'' is also misguided. The practice this Count alleges is unfair is the ''categorization of consumers based on sensitive characteristics derived from location information.'' [14] But there is nothing intrinsically unfair about such categorization, on its own. Instead, each unfairness claim needs to be assessed in a granular way for both substantial injury and countervailing benefits.[15] For example, and contrary to any lop-sided framing of harms concerning abortion:[16]

---

[1] *See, e.g.,* Concurring Statement of Comm'r Melissa Holyoak, *Kochava, Inc.,* FTC Matter No. X230009 (July 15, 2024), *https://www.ftc.gov/system/files/ftc_gov/pdf/2024-7-15-Commissioner-Holyoak-Statement-re-Kochava-final.pdf;* Concurring Statement of Comm'r Melissa Holyoak, Joined In Part By Comm'r Alvaro M. Bedoya (Section I Only), *In re Gravy Analytics, Inc.,* FTC Matter No. 2123035 (Dec. 3, 2024).

[2] *Cf., e.g.,* Dissenting Statement of Comm'r Melissa Holyoak, Joined by Comm'r Andrew N. Ferguson, *In re Rytr, LLC,* FTC Matter No. 2323052, at 1 (Sept. 25, 2024) (''As I have suggested recently in other contexts, the Commission should steer clear of using settlements to advance claims or obtain orders that a court is highly unlikely to credit or grant in litigation. Outside that crucible, the Commission may more readily advance questionable or misguided theories or cases. Nevertheless, private parties track such settlements and, fearing future enforcement, may alter how they act due to a complaint's statement of the alleged facts, its articulation of the law, or how a settlement order constrains a defendant's conduct. In all industries, but especially evolving ones . . . misguided enforcement can harm consumers by stifling innovation and competition. I fear that will happen after today's case, which is another effort by the Majority to misapply the Commission's unfairness authority under section 5 beyond what the text authorizes. Relatedly, I believe the scope of today's settlement is unwarranted based on the facts of this case.'' (citations omitted)), *https://www.ftc.gov/system/files/ftc_gov/pdf/holyoak-rytr-statement.pdf.*

[3] *See* Press Release, *FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices* (Aug. 11, 2022), *https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices.*

[4] *See, e.g.,* Letter from Senator Ted Cruz, Ranking Member, Committee on Commerce, Science, and Transportation, to Lina Khan, Chairwoman, Fed. Trade Comm'n (Nov. 7, 2024) (cautioning that the FTC should ''focus only on matters that are uncontroversial and would be approved unanimously by all Commissioners''); Letter from Representative Jim Jordan, Chairman, Committee on the Judiciary, to Lina Khan, Chair, Fed. Trade Comm'n, at 1 (Nov. 14, 2024) (the ''FTC should also cease all partisan activity''); Letter from Representative Cathy McMorris Rodgers, Chair, Committee on Energy and Commerce, to Lina Khan, Chair, Fed. Trade Comm'n (Nov. 6, 2024) (''As a traditional part of the peaceful transfer of power, the FTC should immediately stop work on any partisan or controversial item under consideration . . . .'').

[5] Accordingly, this case illustrates how leadership at the Commission has vocally claimed to be acting on consumers' behalf over the past several years, but then—where it has effectively usurped the legislative branch—has actually harmed the Commission's legitimacy and long-term ability to serve the American people.

[6] *See* Compl. ¶¶ 9–10.

[7] *Id.*

[8] *Id.* ¶¶ 10, 33.

[9] *See id.* ¶¶ 70–71. The factual predicate appears to be that if the data had never been collected in the first place, consumers could never have been harmed later through its alleged misuse.

[10] *See id.* ¶¶ 7–16, 33–37.

[11] *See* 15 U.S.C. 45(n).

[12] Compl. ¶ 10.

[13] Accordingly, the Commission should not seek to use a novel section 5 theory to support what looks like a remedy for breach of contract, as it does in Provision II of the Order. *See* Provision II (''Prohibition on Collection and Retention of Covered Information from Advertising Auctions'').

[14] Compl. ¶ 69 (emphasis added).

[15] *See, e.g.,* Concurring Statement, *In re Gravy Analytics, supra* note 1, at 6 (''We should not conflate our concern about deceptive advertising (the bogus treatment) *with the lawful act of categorizing and targeting based on sensitive data,* lest we undermine the ability to connect women with life-saving care.'' (emphasis added)). To the extent there is harm here, it could of course stem from wrongful *disclosure* of certain information in certain circumstances—for example, disclosure of location to government agencies circumventing Fourth Amendment protections. But the mere categorization of consumers does not necessarily violate section 5, and it may have significant countervailing benefits.

[16] *Cf.* Compl. ¶¶ 56–57; *see also* Compl., *In re Gravy Analytics,* ¶¶ 67–68 (similar allegations); Compl., *Fed. Trade Comm'n* v. *Kochava, Inc.,* 2:22–cv–00377, ¶¶ 107–08 (D. Idaho, July 15, 2024), ECF No. 86 (similar allegations).

a mother considering her pregnancy may experience significant benefits if data analysis and categorization mean she ultimately receives tailored advertisements from crisis pregnancy centers offering prenatal and postnatal care for her and her child.[17] And a significant benefit would accrue to the unborn child: her survival.[18] Put simply, categorization does not automatically violate section 5. But today's case sends the opposite message.[19]

Count V, for ''Unfair Retention of Consumer Location Information,'' also falls short of what Section 5 requires. The Complaint alleges that Mobilewalla ''indefinitely retains detailed, sensitive information about consumers' movements, including consumers' location information.'' [20] But there is minimal analysis as to how the practice of indefinite retention lacks potential countervailing benefits.[21] For example, as the Complaint makes clear, Mobilewalla facilitates advertising and data analytics.[22] To the extent Mobilewalla's information enables building and optimizing predictive models, or better tailoring advertisements over time to particular consumers, it seems likely Mobilewalla's indefinite retention of data may mean consumers correspondingly experience higher benefits. We will never know whether the practice has net benefits or not, since the Majority simply ignores that step and summarily condemns the practice.

A final point today, about how my approach in this case relates to my support for *Kochava,* where I concurred in filing a second amended complaint. It is one thing to use our unfairness authority to directly address specific acts or practices of ''disclos[ure]'' or ''the revelation of sensitive locations implicating political, medical, and religious activities,'' where there is an appropriate ''focus[ ] on sales of precise geolocation data and related sensitive information,'' [23] and where there has been a lack of consumer consent.[24] The facts pled in *Kochava* relating to disclosure and sale in that case led me to believe that the particular ''act or practice'' of selling precise geolocation data had a direct connection—caused or was likely to cause—substantial injury to consumers.[25]

In contrast, and in focusing on other types of acts or practices—such as the relevant data's collection, its use for categorization, or its indefinite retention—that are analytically removed from and did not themselves necessarily cause any alleged injury based on the facts pled, today's complaint fails to show how these acts or practices themselves satisfy what section 5 requires.[26] On their own, the categorization, collection, or indefinite retention could certainly be factual predicates that precede substantial injury. But, at least as pled in this case, such practices themselves lack the causal connection to substantial injury. And, stepping back, there are certainly innocuous or beneficial instances of related data collection, its categorization, and its indefinite retention. Thus, this case's theories go far beyond the rationale that led me to support amending the complaint in *Kochava.*[27] In fact, the claims in this case seem designed to lead directly to minimizing access to data, limiting the practice of drawing inferences from it, and setting particular boundaries around data retention. This case's regulatory implications are therefore far broader than those in *Kochava.*

Privacy is a vital policy topic. But unless and until the Commission receives new authorities, we must follow the law as Congress actually wrote it, not as some Commissioners or the Bureau Director might amend it if they were elected legislators.[28] Robust enforcement consistent with our statutory authorities can have salutary deterrent effects. But robust enforcement that is inconsistent with our statutory authorities can also have profound ramifications on how markets function, and how market actors proceed—including in ways that harm the American people. And it can undermine our legitimacy in the eyes of not just Congress, but the public.[29] Privacy's tradeoffs should be resolved by Congress, not unelected Commissioners. I do not believe section 5, as drafted, authorizes us to act as a roving legislator, writing law through complaints and settlement orders drafted to suit our purposes or political expediency. I dissent.

[FR Doc. 2024–28745 Filed 12–5–24; 8:45 am]

BILLING CODE 6750–01–P

[17] *See* Concurring Statement, *In re Gravy Analytics, supra* note 1, at 6 (''We also need to disentangle any objections to the content of an advertisement from the practices of categorization and targeting generally.'').

[18] This example illustrates the fraught nature of the Commission determining on its own—without Congressional authorization—what advertising content is harmful, discriminatory, and so on. Absent clear statutory authority, Commission enforcement on such matters becomes a tool driven by preferences of unelected officials.

[19] Compl. ¶ 69 (alleging ''categorization of consumers based on sensitive characteristics for marketing and other purposes is an unfair act or practice'').

[20] *Id.* ¶ 74.

[21] We should be considering such potential benefits, however. *Cf.* Melissa Holyoak, Remarks at National Advertising Division, *A Path Forward on Privacy, Advertising, and AI,* at 6–7, 9 (Sept. 17, 2024), *https://www.ftc.gov/system/files/ftc_gov/pdf/Holyoak-NAD-Speech-09-17-2024.pdf.*

[22] Compl. ¶ 19.

[23] *See* Concurring Statement, *Kochava, supra* note 1, at 2–3.

[24] *Id.* at 3.

[25] *See* 15 U.S.C. 45(n); *see also* Compl., *Fed. Trade Comm'n* v. *Kochava, Inc., supra* note 16, ¶ 132 (bringing a single count for ''Unfair Use and Sale of Sensitive Data,'' and alleging that Defendants ''used and *disclosed* data'' from consumers (emphasis added)). The framing of *Kochava's* unfairness count resembles the framing of the first count in this Complaint against Mobilewalla, for ''unfair sale of sensitive location information,'' related to how Mobilewalla ''sells, licenses, or otherwise transfers precise location information . . . that reveal[s] consumers' visits to sensitive locations.'' *See* Compl. ¶¶ 66–67. But this Complaint's misguided use of the Commission's unfairness authority goes well beyond *Kochava's* sole count.

[26] *See* 15 U.S.C. 45(n).

[27] Again, I ''support[ed filing the second amended complaint in *Kochava*] . . . because I agree[d] that the complaint adequately alleg[d] a likelihood of substantial injury in the revelation of sensitive locations implicating political, medical, and religious activities'' Concurring Statement, *Kochava, supra* note 1, at 2.

[28] *See* Concurring Statement, *In re Gravy Analytics, supra* note 1, at 6 (''As we consider these type of difficult privacy questions in the future, it is of paramount importance that we challenge only unfair or deceptive conduct, supported by specific facts and empirical research, rather than demonizing the entire digital advertising industry. And until Congress acts to address privacy directly through legislation, it is vital we recognize and abide by the limited remit of the Commission's statutory authority.'').

[29] It is no coincidence that the number of constitutional challenges questioning our legitimacy has correlated with the Chair's general dismissal of the Commission's basic norms and integrity. *See, e.g.,* Justin Wise, *FTC's Targets Take Cues From High Court in Tests of Agency Power,* Bloomberg Law (Sept. 26, 2024), *https://news.bloomberglaw.com/antitrust/ftcs-targets-take-cues-from-high-court-in-tests-of-agency-power.*

DEPARTMENT OF DEFENSE

GENERAL SERVICES ADMINISTRATION

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

[OMB Control No. 9000–0007; Docket No. 2024–0053; Sequence No. 19]

Information Collection; Subcontracting Plans

AGENCY: Department of Defense (DOD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA).

ACTION: Notice and request for comments.

SUMMARY: In accordance with the Paperwork Reduction Act of 1995, and