UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of Commissioner
Melissa Holyoak

Concurring Statement of Commissioner Melissa Holyoak
Joined In Part By Commissioner Alvaro M. Bedoya (Section I Only)

Gravy Analytics, Inc., FTC Matter No. 2123035

December 3, 2024

I support today's settlement with two location data broker companies—Respondents Gravy Analytics, Inc. ("Gravy") and its subsidiary, Venntel, Inc. ("Venntel")—to resolve allegations that Respondents: packaged and sold consumers' precise geolocation data to third parties, revealing consumers' visits to places of worship, medical facilities, and political gatherings (Count I); failed to employ reasonable procedures to verify that geolocation data obtained from third parties had been collected with appropriate consumer consent (Count II); and created and sold "audience segments" based on consumers' religious beliefs, political leanings, and medical conditions that had been derived from precise geolocation data (Count III).[1] Staff are to be commended for their efforts and hard work in resolving this matter.

My statement proceeds in two parts: Section I discusses Respondents' collection and sale of consumers' precise geolocation data to third parties and the alleged direct and cognizable harms resulting from that conduct. Section II outlines my views on the necessity, efficacy, and scope of the Proposed Order's injunctive provisions and my interpretation of Count III of the Complaint.

I.

I start by recounting Respondents' alleged conduct here. The Complaint alleges that Respondents collected and purchased vast amounts of consumers' precise geolocation information from third-party data suppliers and mobile applications.[2] Through these various suppliers and applications, Respondents claimed to collect, process, and curate over 17 billion signals from approximately a billion mobile devices on a daily basis.[3] Respondents allegedly packaged and sold this geolocation data—in both raw and enriched formats—along with other persistent identifiers to different commercial entities and government clients.[4] The Complaint also alleges that Gravy separately offered commercial entities curated "audience segments" for targeted advertising, sometimes based on consumers' perceived religious beliefs, political leanings, and medical conditions derived from insights about their geolocation data.[5]

[1] Compl. ¶¶ 76-81.
[2] *Id.* ¶¶ 7-9.
[3] *Id.* ¶ 9.
[4] *Id.* ¶¶ 7, 13-22.
[5] *Id.* ¶¶ 44-45, 50-53.

I am gravely concerned about the potential harms stemming from the sale of consumers' geolocation data,[6] and in certain instances, these harms may constitute a "substantial injury" under Section 5 of the FTC Act.[7] Here, the Complaint alleges that Respondents' sale of consumers' precise geolocation data in certain circumstances enabled their third-party clients to directly track individual consumers' movements at sensitive "geo-fenced" locations, such as places of worship, medical facilities, and political events, with no guardrails or oversight.[8] The Complaint further alleges that this practice directly revealed consumers' political, religious, and medical activities, and thus, constitutes a "substantial injury" under Section 5.[9] I agree. As I explained in the *Kochava* action, selling "precise geolocation information revealing political, medical, or religious activities, without consumers' consent to willing purchasers, . . . breaches [consumers'] trust and jeopardizes Americans' freedoms."[10] Thus, under these circumstances, the alleged sale of consumers' precise geolocation information—data obtained from third-party suppliers without consumers' knowledge and appropriate consent—meets the threshold for alleging "substantial injury" under Section 5.[11]

In addition, consumers' precise geolocation data can be easily misused by law enforcement to impinge on basic freedoms under the United States Constitution, including Americans' Fourth Amendment rights against wrongful government surveillance.[12] I share Commissioner Bedoya's

---

[6] *See, e.g.*, Dhruv Mehrotra & Dell Cameron, *Anyone Can Buy Data Tracking US Soldiers and Spies to Nuclear Vaults and Brothels in Germany*, WIRED (Nov. 19, 2024) ("Experts caution that foreign governments could use [geolocation] data to identify individuals with access to sensitive areas; terrorists or criminals could decipher when [U.S.] nuclear weapons are least guarded; or spies or nefarious actors could leverage embarrassing information for blackmail."), https://www.wired.com/story/phone-data-us-soldiers-spies-nuclear-germany/.

[7] *See* Concurring Statement of Comm'r Melissa Holyoak, *Kochava, Inc.*, FTC Matter No. X230009, at 2 (July 15, 2024) ("I agree that the complaint adequately alleges a likelihood of substantial injury, in the revelation of sensitive locations implicating political, medical, and religious activities. The Commission's effort to protect the privacy of consumers' precise geolocation data in this case correlates to judicial recognition, in other contexts, of how significant such information is."), https://www.ftc.gov/system/files/ftc_gov/pdf/2024-7-15-Commissioner-Holyoak-Statement-re-Kochava-final.pdf.

[8] Compl. ¶¶ 11-12, 16, 18-22, 25-26.

[9] *Id.* ¶¶ 48, 50-53, 56-57, 59.

[10] Holyoak Concurring Statement, *supra* note 7, at 3.

[11] The Complaint alleges several secondary (and indirect) harms that may arise from Respondents' conduct, including "stigma, discrimination, physical violence, emotional distress, and other harms." *See* Compl. ¶¶ 60-69. I have concerns about whether certain secondary harms are legally cognizable, and whether we could meet our burden of proof—at summary judgment or trial—that Respondents' practices raised a "significant risk of concrete harm" to consumers. *Cf. FTC v. Neovi, Inc.*, 604 F.3d 1150, 1157-58 (9th Cir. 2010) ("An act or practice can cause 'substantial injury' by doing a 'small harm to a large number of people, or if it raises a significant risk of concrete harm.'" (citation omitted)); *In re Soc. Media Adolescent Addiction/Pers. Inj. Prod. Liab. Litig.*, No. 4:23-CV-05448-YGR, 2024 WL 4532937, at *29 (N.D. Cal. Oct. 15, 2024) (concluding that the States plausibly alleged a "substantial injury" for Meta's alleged unfair conduct because: (1) "body image and eating disorders" are real medical conditions, (2) "knowingly developing tools that encourage youth addiction 'cannot fairly be classified as either trivial or speculative,'" and (3) the States' allegations present a "substantial risk of imposing at least a 'small harm to a large number of people,' . . . , given these practices are allegedly targeted at all minor users of Facebook and Instagram") (internal citations omitted)). I await guidance from future court decisions, including in the Commission's ongoing *Kochava* litigation, about these harms.

[12] Holyoak Concurring Statement, *supra* note 7, at 2-3 (describing how "government officials can purchase precise geolocation data from commercial data brokers in ways that may circumvent Fourth Amendment protections," and how "[t]here are examples of public-private collaboration in other settings, too, suggesting that government and private-sector entities increasingly work together to leverage consumers' private information without compulsory or formal process, such as a warrant") (citations omitted); *see also id.* at 3 n.12 (citing Lee Fang, *FBI Expands Ability*

concerns about this practice and the harms it poses to Americans.[13] The continued misuse of geolocation data by law enforcement is an ongoing and extant threat to Americans' civil liberties.[14] Moreover, foreign actors can readily purchase precise geolocation data about Americans, including our active-duty military personnel, with no oversight or guardrails, which can pose serious national security and counterintelligence risks.[15]

Although I firmly believe that a comprehensive solution for the sale and disclosure of consumers' geolocation information requires Congressional action,[16] the Commission should not shy away from using all available enforcement tools in the interim to address the evolving practices in the location data broker industry. The Commission should also investigate how location data brokers share geolocation data about Americans with foreign or malign actors. And where the facts warrant it, the Commission should consider stronger injunctive remedies in those cases, including restrictions that prevent or impede the sale of geolocation data about Americans, especially our servicemembers and their families, to bad actors overseas.

II.

I also write separately today to share my views on the Proposed Order's injunctive provisions and my interpretation of Count III of the Complaint (Unfair Sale of Sensitive Inferences Derived from Consumers' Location Data).

To begin with, let me be clear: my vote for today's settlement should not be read as a full-throated endorsement of the Proposed Order in its entirety or every allegation in the Complaint. I have serious concerns about whether the Commission could obtain many of the Proposed Order's injunctive provisions in a contested litigation.[17] Indeed, while the federal district court in the *Kochava* litigation may address the propriety of various types of injunctive relief from the Proposed Order in the coming months, I will continue to reserve judgment here. I also have

---

to Collect Cellphone Location Data, Monitor Social Media, Recent Contracts Show, The Intercept (June 24, 2020), https://theintercept.com/2020/06/24/fbi-surveillance-social-mediacellphone-dataminr-venntel/).

[13] *See* Concurring Statement of Comm'r Alvaro Bedoya, *In re Gravy Analytics, Inc.*, FTC Matter No. 2123035, at § III (Dec. 3, 2024).

[14] *See, e.g.*, H.R. Rep. No. 118-459, pt. 1, at 2 (Apr. 15, 2024) ("H.R. 4639, the Fourth Amendment Is Not For Sale Act . . . closes the legal loophole that allows data brokers to sell Americans' personal information to law enforcement, intelligence agencies, and other government agencies without the agency first acquiring a warrant. If the agency were to gather this information itself, it would be required to obtain a warrant, subpoena, or other legal order. By closing this loophole, the bill prevents government agencies from conducting an end-run around the protections of the Fourth Amendment.").

[15] *Supra* note 6.

[16] *See generally* H.R. 4639, Fourth Amendment Is Not For Sale Act, § 2 ("A law enforcement agency of a governmental entity and an element of the intelligence community may not obtain from a third party in exchange for anything of value a covered customer or subscriber record or any illegitimately obtained information."); H.R. 815, Pub. L. No. 118-50, Division I, Protecting Americans' Data from Foreign Adversaries Act of 2024, § 2 ("It shall be unlawful for a data broker to sell, license, rent, trade, transfer, release, disclose, provide access to, or otherwise make available personally identifiable sensitive data of a United States individual to—(1) any foreign adversary country; or (2) any entity that is controlled by a foreign adversary.").

[17] *See, 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."), https://www.ftc.gov/system/files/ftc_gov/pdf/holyoak-rytr-statement.pdf.

questions about the necessity and efficacy of the injunctive provisions found in Sections VI, VII, and IX,[18] which first appeared in the *X-Mode Social* matter before my arrival at the Commission.[19] As we turn the page on the last four years, the Commission should comprehensively examine the utility of the type of injunctive relief found in today's Proposed Order in the future and implement changes where warranted.[20]

A. Proposed Order.

While today's settlement is not perfect by any measure, several provisions in the Proposed Order will mitigate the harms resulting from Respondents' allegedly unlawful practices—*i.e.*, the disclosure of consumers' political, religious, and medical activities. Critically, the Proposed Order will prohibit the unauthorized sale or disclosure of "Sensitive Location Data"—geolocation data associated with military installations and buildings, medical facilities, religious organizations, childcare and education services, and many others—to third parties.[21] It also requires Respondents to implement a "Sensitive Data Location" program, as well as prophylactically avoid associating consumers' precise geolocation data with (1) political demonstrations, marches, and protests and (2) residences for individual consumers.[22] The Proposed Order further requires Respondents to offer individual consumers the ability to request deletion of their geolocation data in Respondents' datasets.[23]

[18] For example, these injunctive provisions collectively require Respondents to ensure that consumers have affirmatively consented to all upstream uses of their location data, such as for targeted advertising, and provide opt-out mechanisms for consumers to withdraw consent directly with Respondents, even though Respondents "do not collect mobile location data directly from consumers" and consumers "have no interactions with Respondents and have no idea that Respondents have obtained their location data." Compl. ¶ 8; *see generally* Proposed Decision and Order §§ VI (Limitations on Collection, Use, Maintenance, and Disclosure of Location Data), VII (Supplier Assessment Program), and IX (Withdrawing Consent). I question the efficacy of these provisions given their focus on Respondents, which are upstream from the initial collection of this data from consumers. While ensuring appropriate consent for all upstream uses of consumers' data is laudable goal, the Commission may be better served by focusing injunctive relief on the companies that collect this data in the first instance, not upstream data aggregators like Respondents.

[19] *Compare* Proposed Decision and Order §§ VI (Limitations on Collection, Use, Maintenance, and Disclosure of Location Data), VII (Supplier Assessment Program), and IX (Withdrawing Consent) *with In re X-Mode Social, Inc. and Outlogic, LLC,* FTC Matter No. 212-3038, Proposed Decision and Order §§ VI-VII, IX (Jan. 9, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/X-Mode-D%26O.pdf.

[20] During the first Trump administration, the Commission held several public hearings on Competition and Consumer Protection in the 21st Century, including to solicit public and industry feedback on improvements to the Commission's data security orders. *See* Hearings on Competition & Consumer Protection in the 21st Century, Fed. Trade Comm'n (2018-19), https://www.ftc.gov/enforcement-policy/hearings-competition-consumer-protection. Following these public hearings, the Commission updated its data security orders, and FTC staff explained the key changes in public-facing guidance. *See* Andrew Smith, Former Director of the Bureau of Consumer Protection, *New and Improved FTC Data Security Orders: Better Guidance for Companies, Better Protection for Consumers,* FTC BUSINESS BLOG (Jan. 6, 2020), https://www.ftc.gov/business-guidance/blog/2020/01/new-and-improved-ftc-data-security-orders-better-guidance-companies-better-protection-consumers.

[21] Proposed Decision and Order § II; *see also id.* at 2 (Definitions).

[22] *See id.* §§ III-IV. Indeed, I believe the Proposed Order's terms will prevent some of the unfortunate public-private partnerships we have seen recently in the context of political activity. *See, e.g.*, Holyoak Concurring Statement, *supra* note 7, at 3 n.13.

[23] Proposed Decision and Order § XI.

I support Sections II, III, IV, and XI of the Proposed Order since they are directly tied to Respondents' alleged conduct, help mitigate the specific harms from disclosing consumers' political, religious, and medical activities, and properly balance the costs and benefits, as required by Section 5 of the FTC Act. But today's settlement also has important limits, particularly with the sale and use of "Sensitive Location Data". In my view, the Proposed Order strikes the proper balance under our unfairness authority. Permitting the use and disclosure of precise geolocation information to third parties for national security or data security purposes,[24] or to prevent imminent risk of death or serious bodily harm,[25] presents tangible benefits that appropriately fall within the confines of the Proposed Order's carefully negotiated definitions.

At the same time, the Proposed Order's restrictions on further disclosure of consumers' geolocation data help protect American citizens' constitutional rights under the Fourth Amendment of the United States Constitution. Fourth Amendment rights should not be for sale, under any circumstance. I agree with Commissioner Bedoya on this issue and the importance of the Proposed Order's restrictions here.[26] Constitutionally appropriate process, such as warrants or subpoenas, exists for law enforcement to obtain information it needs, without resorting to purchasing consumers' precise geolocation data from unscrupulous location data brokers to circumvent judicial oversight.[27] Nor does the Proposed Order have a deleterious impact on law enforcement efforts. Law enforcement personnel can always avail themselves of the appropriate legal process to obtain such data in a manner that comports with Fourth Amendment requirements.

B. Count III (Unfair Sale of Sensitive Inferences)

The Complaint alleges that Gravy created and sold custom "audience segments" based on consumers' religious beliefs, political leanings, and medical conditions by geo-fencing sensitive locations, such as breast cancer events, specific churches, and "Republican focused political events."[28] The sale of "audience segments" tied to consumers' religious beliefs, political leanings, and medical conditions qualifies as an unfair practice: it "causes or is likely to cause substantial injury" by revealing consumers' political, religious, and medical activities (as discussed *supra* in Section I), consumers cannot reasonably avoid the harm (they are not aware of Respondent and did not consent to the use), and it is not outweighed by any countervailing benefits to consumers or competition.[29] For these reasons, I support Count III.

However, my vote today does not entail broader support for the Majority's continued effort to deem targeted advertising an unfair practice under Section 5. Nor should my vote be construed

[24] *See* Proposed Decision and Order at 4 (defining "National Security" to mean "the national defense, foreign intelligence and counterintelligence, international and internal security, and foreign relations[,]" which "includes countering terrorism; combating espionage and economic espionage conducted for the benefit of any foreign government, foreign instrumentality, or foreign agent; enforcing export controls and sanctions; and disrupting cyber threats that are perpetrated by nation states, terrorists, or their agents or proxies").
[25] *Id.* at 4 (defining "Location Data" to exclude data used for "National Security" purposes, "Security Purposes," and "response by a federal law enforcement agency to an imminent risk of death or serious bodily harm to a person").
[26] Bedoya Concurring Statement, *supra* note 13, at § IV.
[27] Holyoak Concurring Statement, *supra* note 7, at 2-3.
[28] Compl. ¶¶ 50-53.
[29] *Id.* ¶¶ 56-59.

as endorsing the Complaint's theory about secondary harm to consumers.[30] As I have explained before, we must "tease out the complexity of the privacy debate" and "press for more empirical research" to ground our unfairness analysis.[31] Our complaints cannot simply rely on politically charged buzzwords. For example, the Complaint here expresses concerns with Gravy's practice of creating general "audience segments" for targeted advertising—e.g., "Sports Betting Enthusiast[s]," "Early Risers," "Healthy Dads," "New Parents", or "Parents with Young Kids"[32] But the Complaint fails to confront how these audience segments create a "significant risk of concrete harm" and ignores the potential benefits to consumers and competition. Behaviorally targeted advertising may produce more relevant ads to consumers, reducing their search costs and allowing small businesses and new market entrants to connect with a broader consumer base.[33]

Moreover, my vote should not be construed as support for deeming the use of sensitive data or the categorization of sensitive data as unlawful in every circumstance. Consumers may be deceived or harmed where their sensitive data is used without their knowledge or consent, contrary to their reasonable expectations. But context matters. For example, if a consumer searches online for nearby pediatricians close to their home, then serving ads in other contexts for pediatrician offices and groups based on the consumer's location may be both reasonable and desirable. If a consumer subscribes to a podcast on a certain type of politics, advertisements for other political podcasts may be of interest to that consumer.

We also need to disentangle any objections to the content of an advertisement from the practices of categorization and targeting generally. Take, for example, the practice of categorizing consumers into the ad segment "women over 50 suffering from breast cancer." An advertiser may use that segment to target ads for well-validated treatments, potentially connecting women with life-saving care. Or, an advertiser could use that segment to target ads for bogus treatments. 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. This is just one example of the potentially beneficial or harmful content served to audience segments. Certain types of categorization and targeting may offer similar benefits to consumers and competition, if used properly and in a lawful manner.[34]

As we consider these types 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.[35] 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.

---

[30] *Id.* ¶¶ 60-69.
[31] Melissa Holyoak, Remarks at National Advertising Division, *A Path Forward on Privacy, Advertising, and AI*, at 7 (Sept. 17, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/Holyoak-NAD-Speech-09-17-2024.pdf.
[32] Compl. ¶¶ 47-49.
[33] *See, e.g.*, Commissioner Holyoak Remarks, *supra* note 31, at 6.
[34] *See generally* Concurring and Dissenting Statement of Comm'r Melissa Holyoak, *Social Media and Video Streaming Services Staff Report*, Matter No. P205402, at 15-18 (Sept. 19, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/commissioner-holyoak-statement-social-media-6b.pdf.
[35] Commissioner Holyoak Remarks, *supra* note 31, at 5-7.