based on such factors; or (3) about the accuracy or efficacy of its Facial Recognition Technology with respect to detecting spoofing or otherwise determining Liveness. (Facial Recognition Technology and Liveness are defined in the Proposed Order.)

Provision II prohibits Respondent from making any representation about the effectiveness, accuracy, or lack of bias of Facial Recognition Technology, or about the effectiveness of such Facial Recognition Technology at detecting spoofing, unless Respondent possesses and relies upon competent and reliable testing that substantiates the representation at the time the representation is made. For the purposes of this Provision, competent and reliable testing means testing that is based on the expertise of professionals in the relevant area, and that (1) has been conducted and evaluated in an objective manner by qualified persons and (2) is generally accepted by experts in the profession to yield accurate and reliable results. Respondent also must document all such testing including: the dates and results of all tests; the method and methodology used; the source and number of images used; the source and number of different people in the images; whether such testing includes Liveness tests; any technique(s) used to modify the images to create different angles, different lighting conditions or other modifications; demographic information collected on images used in testing if applicable; information about the skin tone collected on images used in testing if applicable; and any information that supports, explains, qualifies, calls into question or contradicts the results. Provision III requires Respondent to obtain and submit acknowledgments of receipt of the Order.

Provisions IV–VI are reporting and compliance provisions, which include recordkeeping requirements and provisions requiring Respondent to provide information or documents necessary for the Commission to monitor compliance. Provision VII states 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.

April J. Tabor,

Secretary.

Concurring Statement of Commissioner Andrew N. Ferguson

Today, the Commission approves a complaint and settlement against IntelliVision, a developer of facial recognition software.[1] Count I charges IntelliVision with misrepresenting the efficacy of its software. IntelliVision claimed that its software had one of the highest accuracy rates in the world, but in reality it was not even among the top hundred best performing algorithms tested by the National Institute of Standards and Technology.[2] Count I further accuses IntelliVision of claiming that its software was trained on ''millions'' of faces, when the software was in fact trained on only 100,000 faces.[3] Count III accuses IntelliVision of claiming that its software could not be fooled by photo or video images even though it had insufficient evidence to support that categorical claim.[4] I support these counts without reservation.

I write briefly to explain why I also support Count II, which accuses IntelliVision of misrepresenting that its software performs with ''zero gender or racial bias'' when in fact its software exhibits substantially different false-negative and false-positive rates across sex and racial lines.[5] Treating IntelliVision as having committed a deceptive act or practice in these circumstances could lead one to believe that the Commission is taking the position that to be ''unbiased,'' a software system must produce equal false-negative and false-positive rates across race and sex groups.

I do not read the complaint that way, and I today do not vote to fix the meaning of ''bias.'' Statistical disparity in false-positive and false-negative rates is not necessarily the only or best definition of what it means for an automated system to be ''biased.'' The question is open to philosophical and political dispute. Other definitions might consider the discriminatory intentions of the developers, the developers' diligence in avoiding artificial disparities while training the automated system, or whether any statistical disparities reflect the underlying realities the system is designed to reflect or epistemological limitations in that underlying reality that are impossible or uneconomical to overcome. This complaint does not choose from among these competing definitions and considerations.

But IntelliVision used the word ''bias.'' If it intended to invoke a specific definition of ''bias,'' it needed to say so. But it did not say so; it instead left the resolution of this ambiguity up to consumers. IntelliVision must therefore bear the burden of substantiating all reasonable interpretations that consumers may have given its claim that its software had ''zero gender or racial bias.'' [6] A reasonable consumer could interpret ''zero gender or racial bias'' in this context to mean equal rates of false positives and false negatives across those lines. I therefore have reason to believe that IntelliVision's claims were false or unsubstantiated because its software did not have equal false-positive and false-negative rates across those lines.

Pursuant to that understanding, I concur in the filing of the complaint and settlement.

[FR Doc. 2024–28716 Filed 12–5–24; 8:45 am]

BILLING CODE 6750–01–P

[1] Complaint, *In re IntelliVision Technologies Corp.*

[2] *Id.* ¶ 11.

[3] *Id.* ¶ 14.

[4] *Id.* ¶ 13.

[5] *Id.* ¶ 11.

[6] FTC Policy Statement on Deception, 103 F.T.C. 174, 178 (1984) (''When a seller's representation conveys more than one meaning to reasonable consumers, one of which is false, the seller is liable for the misleading interpretation''); FTC Policy Statement Regarding Advertising Substantiation, 104 F.T.C. 839, 840 (1984) (''Although firms are unlikely to possess substantiation for implied claims they do not believe the ad makes, they should generally be aware of reasonable interpretations and will be expected to have prior substantiation for such claims. The Commission will take care to assure that it only challenges reasonable interpretations of advertising claims.'').

FEDERAL TRADE COMMISSION

[File No. 212 3035]

Gravy Analytics, 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 ''Gravy Analytics; File No. 212 3035'' 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 G), Washington, DC 20580.

FOR FURTHER INFORMATION CONTACT: Jennifer Rimm (202–326–2277), Attorney, 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 ''Gravy Analytics; File No. 212 3035'' 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 ''Gravy Analytics; File No. 212 3035'' 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 G), 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 Gravy Analytics, Inc. (''Gravy Analytics'') and Venntel, Inc. (''Venntel,'' and collectively with Gravy Analytics, ''Respondents''). 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.

Gravy Analytics and Venntel are Delaware corporations with their headquarters in Virginia. Respondent Venntel is a subsidiary of Gravy Analytics. Gravy Analytics and Venntel are data brokers that collect and sell precise geolocation data about consumers' mobile devices.

Gravy Analytics does not collect data directly from consumers. Rather, it purchases precise geolocation data and other personal data for its products from other data suppliers, including other data aggregators. Gravy Analytics offers several data products to its customers. These products include transfers of batch location data, consisting of a unique persistent identifier for the mobile device called a Mobile Advertiser ID (''MAID'') and timestamped latitude and longitude coordinates; audience segments, which are groupings of MAIDs that purportedly share similar traits based on the locations or events the mobile devices and MAIDs have visited; and an online application programming interface that, among other things, enables Gravy Analytics' customers to geofence locations. Gravy Analytics makes its data products available to commercial customers, such as marketers, other data brokers, stores, and other commercial entities.

Venntel obtains mobile location data from Gravy Analytics exclusively. Venntel offers batch transfers of location data and allows customers to geofence specific locations. Venntel also offers its customers access to an online application programming interface through which its customers may search for devices that visited specific

locations, obtain device information about a particular mobile phone, or obtain location data for individual devices. Venntel sells its data products only to public sector customers, such as government contractors.

The Commission's proposed three-count complaint alleges Respondents violated section 5(a) of the FTC Act by (1) unfairly selling sensitive location data and (2) unfairly collecting, using, and transferring consumer location data without consent verification; and that Gravy Analytics violated section 5 of the FTC Act by (3) unfairly selling inferences about consumers' sensitive characteristics derived from location data.

With respect to the first count, the proposed complaint alleges Respondents sold location data associated with persistent identifiers, such as MAIDs, that could be used to track consumers to sensitive locations, such as medical facilities, places of religious worship, places that may be used to infer an LGBTQ+ identification, domestic abuse shelters, and welfare and homeless shelters. For example, by plotting timestamped latitude and longitude coordinates associated with mobile devices using publicly available map programs, it is possible to identify which consumers' mobile devices visited medical facilities and when.

With respect to the second count, the proposed complaint alleges Respondents failed to verify that their data suppliers obtained informed consent from consumers to have the consumers' location data collected, used, and sold. Respondents' primary mechanism for ensuring that consumers have provided appropriate consent is through contractual requirements with their suppliers. However, contractual provisions, without additional safeguards, are insufficient to protect consumers' privacy.

With respect to the third count, the proposed complaint alleges it was an unfair practice for Gravy Analytics to sell inferences about consumers' sensitive characteristics derived from their location data. Gravy Analytics created custom audience segments for customers based, for example, on consumers' attendance at a cancer charity run and based on consumers' church attendance, and has also offered standard audience segments based on medical decisions and political activities.

The proposed complaint alleges that Respondents could have addressed each of these failures by implementing certain safeguards at a reasonable cost and expenditure of resources. The proposed complaint alleges Respondents' practices caused, or are likely to cause, substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves. Such practices constitute unfair acts or practices under section 5 of the FTC Act.

The Proposed Order contains injunctive relief designed to prevent Respondents from engaging in the same or similar acts or practices in the future. Part I prohibits Respondents from misrepresenting the extent to which: (1) Respondents review data suppliers' compliance and consent frameworks, consumer disclosures, sample notices, and opt in controls; (2) Respondents collect, maintain, use, disclose, or delete any covered information, and (3) the location data that Respondents collect, use, maintain, or disclose is deidentified.

Part II prohibits Respondents from selling, licensing, transferring, sharing, disclosing, or using sensitive location data in any products or services. Sensitive locations are defined as those locations in the United States 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 of entities held out to the public as predominantly providing education or childcare services to minors; (6) associations held out to the public as predominantly providing services based on racial or ethnic origin; (7) locations held out to the public as providing temporary shelter or social services to homeless, survivors of domestic violence, refugees, or immigrants; or (8) military installations, offices, or buildings. This prohibition does not apply to sensitive location data used to respond to or prevent data security incidents, for national security purposes conducted by Federal agencies or other Federal entities, or for response by a Federal law enforcement agency to an imminent risk of death or serious bodily harm to a person. Part III requires that Respondents implement and maintain a sensitive location data program to develop a comprehensive list of sensitive locations and to prevent the use, sale, license, transfer, sharing, or disclosure of sensitive location data.

Part IV requires that Respondents establish and implement policies, procedures, and technical measures designed to prevent recipients of Respondents' location data from associating consumers with locations predominantly providing services to LGBTQ+ individuals, locations of public gatherings of individuals during social demonstrations, marches, or protests, or using location data to determine the identity or location of an individual's home. Part V requires that Respondents notify the Commission any time Respondents determine that a third party shared Respondents' location data, in violation of a contractual requirement between Respondents and the third party.

Part VI requires that Respondents must not collect, use, maintain, and disclose location data: (1) when consumers have opted-out, or otherwise declined targeted advertising and (2) without a record documenting the consumer's consent obtained prior to the collection of location data. Part VII requires that Respondents implement a supplier assessment program designed to ensure that consumers have provided consent for the collection and use of all data obtained by Respondents that may reveal a consumer's precise location. Under this program, Respondents must conduct initial assessments of all their data suppliers within 30 days of entering into a data sharing agreement, or within 30 days of the initial date of data collection. The program also requires that Respondents confirm that consumers provided consent and create and maintain records of suppliers' assessment responses. Finally, Respondents must cease from using, selling, or disclosing location data for which consumers have not provided consent.

Part VIII requires that Respondents provide a clear and conspicuous means for consumers to request the identity of any entity, business, or individual to whom Respondents know their location data has been sold, transferred, licensed, or otherwise disclosed or a method to delete the consumers' location data from the databases of Respondents' customers. Respondents must also provide written confirmation to consumers that the deletion requests have been sent to Respondents' customers.

Part IX requires that Respondents provide a simple, easily-located means for consumers to withdraw any consent provided and Part X requires that Respondents cease collecting location data within 15 days after Respondents receive notice that the consumer withdraws their consent. Part XI also

requires that Respondents provide a simple, easily-located means for consumers to request that Respondents delete location data that Respondents previously collected and to delete the location data within 30 days of receipt of such request unless a shorter period for deletion is required by law.

Part XII requires that Respondents: (1) document and adhere to a retention schedule for the covered information they collect from consumers, including the purposes for which they collect such information, the specific business needs, and an established timeframe for its deletion, and (2) prior to collecting or using any new type of information related to consumers that was not previously collected, and is not described in its retention schedule, Respondents must update their retention schedules. Part XIII requires that Respondents delete or destroy all historic location data and all data products developed using this data. Respondents have the option to retain historic location data if they have records showing they obtained consent or if they ensure that the historic location data is deidentified or rendered non-sensitive. Respondents must inform all customers that received location data from Respondents within 3 years prior to the issuance date of this Order of the Commission's position that such data should be deleted, deidentified, or rendered non-sensitive. Part XIV requires Respondents to establish and implement, and thereafter maintain, a comprehensive privacy program that protects the privacy of consumers' personal information.

Parts XV–XVIII are reporting and compliance provisions, which include recordkeeping requirements and provisions requiring Respondents to provide information or documents necessary for the Commission to monitor compliance. Part XIX 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 Ferguson dissenting.

April J. Tabor,

Secretary.

Statement of Commissioner Alvaro M. Bedoya Joined by Chair Lina M. Khan and Commissioner Rebecca Kelly Slaughter in Full and Commissioner Melissa Holyoak in Part I

I. The Porous Line Between Government and Private Surveillance

Any first-year constitutional law student will tell you that the distinction between a government agent and private actor is paramount: the Fourth Amendment corrals the former but not the latter. For the people being watched, that line is porous if not irrelevant.

Governments have long relied on private citizens for work that would be impractical or illegal for law enforcement. Elizabeth I prided herself on seeing and hearing all in her realm, famously sitting for one of her final portraits in a gown embroidered with human eyes and ears.[1] Her ministers achieved that surveillance through a much-feared system of agents and spies,[2] as well as a quieter network of local clergy who tracked the weekly church attendance of converted Catholics and the Separatist Puritans we now know as Pilgrims.[3] Her successor, James I, went further, offering bounties to any of his subjects who reported practicing Catholics.[4]

The governor of Plymouth Colony, William Bradford, would later recount what forced him and his fellow migrants to travel, first to the Netherlands and then to the New World. They were ''hunted & persecuted on every side,'' he wrote. While ''some were taken & clapt up in prison, others had their houses besett & watctht night and day[.]'' [5]

Four-hundred years later, those loose networks of citizen-informants have been succeeded by a digitized, automated, and highly profitable industry of commercial data brokers that ''artfully dodge[ ] privacy laws.'' [6] In 2001, the Electronic Privacy Information Center used the Freedom of Information Act to survey Federal law enforcement agencies' reliance on those firms.[7] They determined that this network of data brokers allows law enforcement to easily and warrantlessly ''download comprehensive dossiers on almost any adult.'' [8] They warned that ''[i]f we are ever unfortunate enough to have George Orwell's Big Brother in the United States, it will be made possible by the private sector.'' [9]

This complaint and proposed settlement concern two contemporary peers of those data brokers, Gravy Analytics, Inc. and its subsidiary, Venntel, Inc. (''Respondents''). The Commission alleges these companies collect, aggregate, and sell precise geolocation data from roughly one billion mobile devices.[10] According to public reporting, Venntel's customers have included American law enforcement.[11]

[1] *See generally* Daniel Fischlin, *Political Allegory, Absolutist Ideology, and the ''Rainbow Portrait'' of Queen Elizabeth I,* 50 Renaissance Q. 170, 175–83 (1997) (reflecting the view that the portrait was intended to convey that ''[t]he Queen watches and listens vigilantly, seeing in all perspectives, hearing in all directions'').

[2] *See generally* John Coffey, Persecution and Toleration in Protestant England, 1558–1689 (2000). *See also id* at 95–96 (describing government agents loitering in St. Paul's courtyard ''pretending to be sympathetic'' to the Puritans' cause); Stephen Budiansky, *Sir Francis Walsingham,* Brittanica, *available at https://www.britannica.com/biography/Francis-Walsingham* (last accessed Nov. 29, 2024).

[3] *See* Act of Uniformity, 1 Eliz. 1, c. 2 (1559) (instituting a 12 shilling fine for absences, ''to be levied by the churchwardens of the parish where such offence shall be done''); An Act to retain the Queen's Majesty's Subjects in their due Obedience, 23 Eliz. 1, c. 1 (1580) (raising the fine to 20 pounds); Act Against Puritans, 35 Eliz. 1, c. 1 (1593) (instituting penalties for Puritans who profess allegiance to the Church of England, only to subsequently fail to attend church services).

[4] *See* An Act to Prevent and Avoid Dangers which Grow by Popish Recusants, 3 Jas. 1, c. 5 (1605) (immunizing informants and providing them one-third of the money seized from the offending individual).

[5] *See* William Bradford, Of Plymouth Plantation 6 (c. 1630–1651). Professor Coffey explains that, while Catholics were the focus of government surveillance efforts at the time, Separatist Puritans were also targeted. *See* Coffey, *supra note* 2, at 103 (''The harsh repression of the Separatists in the 1580s and 90s was. . . out of all proportion to their threat. [. . .] Separatist congregations were hunted down and incarcerated, their ringleaders put to death.'').

[6] *See* Chris J. Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement,* 29 N.C. J. Int'l L. 595, 595 (2003).

[7] *Id.* at 597.

[8] *Id.* at 595.

[9] *Id.* at 633.

[10] Complaint, *FTC* v. *Gravy Analytics, Inc. & Venntel, Inc.,* (Dec. 2, 2024), [hereinafter *Complaint*] at 2.

[11] *See, e.g.,* Byron Tau and Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement,* Wall Street Journal, (Feb. 7, 2020), *https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600;* Joseph Cox, *The DEA Abruptly Cut Off Its App Location Data Contract, Vice*, (Dec. 7, 2020), *https://www.vice.com/en/article/dea-venntel-location-data/;* Lee Fang, *FBI Expands Ability to Collect Cellphone Location Data, Monitor Social Media, Recent Contracts Show,* The Intercept, (Jun. 24, 2020), *https://theintercept.com/2020/06/24/fbi-surveillance-social-media-cellphone-dataminr-venntel/;* Byron Tau, *IRS Used Cellphone Location Data to Try to Find Suspects, Wall Street Journal*, (Jun. 19, 2020), *https://www.wsj.com/articles/irs-used-cellphone-location-data-to-try-to-find-suspects-11592587815.*

II. The Respondents' Privacy Invasions Clearly Violate Section 5 of the FTC Act

You may not know anything about Gravy Analytics, but Gravy Analytics may know quite a bit about you.

Do you eat breakfast at McDonald's? Do you buy CBD oil? Did you recently buy lingerie? Are you pregnant? Are you a stay-at-home parent? Are you a Republican? A Democrat? Are you in the pews every Sunday in Charlotte? Or Atlanta? Have you recently attended an event for breast cancer? Are you a blue-collar Gen X parent and golf-lover who has recently been looking into Medicare?

These are just a few of the 1,100 labels that the Commission alleges that Gravy Analytics appended to individual consumers so as to sell their bundled data to private companies for targeted advertising—or to better understand the ''persona'' of any given individual whose data a company has requested.[12] According to our complaint, Respondents actively encouraged their customers to identify individual people using the data they sold.[13]

In the complaint, the Commission alleges that the Respondents' 1) sale of data tying consumers to sensitive locations, (2) collection and use of geolocation data without verifying that it was obtained with consumers' informed consent, and (3) the sale of sensitive inferences about those consumers' ''medical conditions, political activities, and religious beliefs,'' among other things, constitute unfair trade practices prohibited by section 5 of the Federal Trade Commission Act.

I agree with my colleague Commissioner Holyoak that the specific practices alleged in the complaint meet the threshold for ''substantial injury'' under section 5.[14] More than a decade ago, the Commission issued a final report offering guidance to businesses on protecting the privacy of American consumers.[15] That report classified ''precise geolocation'' as a type of ''sensitive information,'' and urged companies to obtain people's affirmative express consent before collecting it.[16] As the District Court of Idaho affirmed last year, collection and disclosure of precise geolocation is a violation of privacy—itself an injury.[17] It can further lead to stigma, harassment, and even physical danger.[18]

This is the fourth recent Commission action and third settlement brought to stop the nonconsensual collection and sale of geolocation data.[19] In my view, the illegality of this conduct is more than clear.

III. Venntel's Sales of Location Data Undermine Established Fourth Amendment Protections

According to our complaint, Respondent Venntel ''markets to its public sector customers that the location data and these enhanced tools can be used for government purposes.'' [20] Public reporting suggests that these government clients have included Federal law enforcement agencies like the Department of Homeland Security (DHS), the Drug Enforcement Administration (DEA), the Federal Bureau of Investigation (FBI), and the Internal Revenue Service (IRS).[21] This poses an important question: Can a collection of precise geolocation data that otherwise violates section 5 be cured by a potential future law enforcement use of that data?

I think the answer is ''no.'' Section 5 makes no mention of such a circumstance, but it does expressly call on the Commission to consider ''countervailing benefits to consumers'' from the practice in question, and further permits the Commission to weigh ''established public policies as evidence to be considered with all other evidence'' when declaring a practice unfair.[22]

In 1928, Justice Louis Brandeis, one of the architects of this Commission, warned against formalistic interpretations of the Fourth Amendment. ''Clauses guaranteeing to the individual protection against specific abuses of power must have a . . . capacity of adaptation to a changing world,'' he wrote.[23] For the last 60 years, since the *Katz* court's declaration that the Fourth Amendment ''protects people, not places,'' the Supreme Court has more or less heeded that call.[24]

In *Kyllo,* the Court found that a thermal imaging device that allowed law enforcement to track activities inside a home constituted a search under the Fourth Amendment—even though it involved no trespass into the home.[25] In *Riley,* the Court refused to equate the search of someone's cellphone with searches of their purse or wallet or any other physical items people carry.[26] Most relevantly, in *Carpenter,* the Court held that citizens have a reasonable expectation of privacy in extended cell-site location records of their movements, irrespective of the fact that the data accessed by the government was disclosed to and held by a commercial third party, and further held that the government must generally obtain a warrant before acquiring such records.[27]

Look at the cell-site location data in *Carpenter;* look at the data in question here. It's basically the same data. In some ways, the Respondents' data is more invasive.

The cell-site records in *Carpenter* could place an individual ''within a wedge-shaped sector ranging from one-eighth to four square miles''; [28] Respondents' data locates people down to a meter.[29] Cellphone carriers maintain location records for five years, and Federal agents obtained a total of 129 days of geolocation data—although the Court held that accessing just seven days of data constitutes a Fourth Amendment search.[30] The Respondents can draw on three years of data, and Venntel offers its clients the ability to ''continuously'' track a person's phone for 90 days.[31] The *Carpenter* court warned that cell-site geolocation records

[12] *See* Complaint, *supra* note 10, at 9–10.

[13] *Id.* at 5.

[14] Statement of Commissioner Melissa Holyoak, In the Matter of Gravy Analytics, Inc. & Venntel, Inc. (Dec. 2, 2024).

[15] Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, (2012).

[16] *Id.* at 58.

[17] *See* Order on Motion to Dismiss, *FTC* v. *Kochava, Inc.,* 2:22–cv–00377–BLW, (D. Idaho May 4, 2023) at 8–10, (''an invasion of privacy may constitute an injury that gives rise to liability under Section 5(a)'') *https://www.ftc.gov/system/files/ftc_gov/pdf/71-OpinionMTD.pdf.*

[18] *Id.* at 8–9.

[19] Complaint, *FTC* v. *Kochava, Inc.,* 2:22–cv–00377–BLW, (D. Idaho Jul. 15, 2024), *https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf;* Complaint, *FTC* v. *X-Mode Social, Inc.,* Docket No. 212–3038, (Jan. 9, 2024), *https://www.ftc.gov/system/files/ftc_gov/pdf/X-Mode-Complaint.pdf;* Complaint, *FTC* v. *InMarket Media, LLC,* Docket No. 202–3088, (Jan. 18, 2024), *https://www.ftc.gov/system/files/ftc_gov/pdf/Complaint-InMarketMediaLLC.pdf.*

[20] Complaint, *supra* note 10.

[21] *See supra* note 11.

[22] 15 U.S.C. 45(n). To be clear, I do not believe that an appeal to public policy is necessary to support this matter. Still, I believe it is useful exercise here, especially when considering the Commission's actions relative to other policy priorities.

[23] *Olmstead* v. *United States,* 277 U.S. 438, 472 (Brandeis, J., dissenting). The *Olmstead* majority held that a prolonged wiretap did not constitute a search or seizure for the purposes of the Fourth Amendment because the interception occurred along public phone lines leading to the home in question—''[t]here was no entry of the houses or offices of the defendants.'' *Id.* at 464.

[24] *Katz* v. *United States,* 389 U.S. 347, 351 (1967).

[25] *Kyllo* v. *United States,* 533 U.S. 67 (2001).

[26] *Riley* v. *California,* 573 U.S. 373 (2014).

[27] *See Carpenter* v. *United States,* 585 U.S. 296, 306–321 (2018).

[28] *See Carpenter,* 585 U.S. at 312.

[29] Complaint, *supra* note 10, at 2.

[30] *See Carpenter,* 585 U.S. at 302 (129 days) & 310 n. 3 (seven days constitutes a Fourth Amendment search).

[31] Complaint, *supra* note 10, at 3–4.

can reveal a person's ''familial, political, professional, and sexual associations''—a phrase that might as well be Respondents' marketing slogan.[32]

To make this plain: *Carpenter* said that to get this data, you need a warrant; Venntel lets them get it without a warrant. I cannot see how this is a ''countervailing benefit to consumers.'' It certainly contravenes ''established public policy.''

Looking beyond *Carpenter,* a panoply of statutes sets out a range of safeguards against the government's untrammeled collection of Americans' sensitive data. The Wiretap Act requires warrants to authorize wiretapping and interception of communications.[33] The Stored Communications Act protects the privacy of subscribers' information held by internet service providers and established procedures for government access by warrant, subpoena, court order, or written consent.[34]

Both of those laws concern oral or written communications; one may assume that Congress would want to protect this data. Consider that if law enforcement wants YouTube to disclose the name of a single video that I have watched online, Federal statute requires that they get a warrant, grand jury subpoena, or a court order.[35] Similarly, the Cable Act provides that cable subscribers' personally identifiable information, such as their viewing habits, cannot be disclosed without their consent, except in the case of a court order.[36]

Admittedly, there is active debate around whether these statutes impose the correct degree of protection in light of the Fourth Amendment. That said, the correct degree is clearly not zero.

IV. The Proposed Order

Speaking generally, the proposed order prohibits Respondents from disclosing sensitive location data in any of its products or services.[37] Sensitive location data includes, *inter alia,* medical facilities, religious buildings, schools and daycares, domestic violence shelters, and military facilities.[38] The order also directs Respondents to ensure that their clients do not use their data to track people to political protects, or to locate someone's home.[39] The order requires that Respondents not collect any data from consumers that have opted out of targeted advertising via their operating system, and will block them from collecting, using, or disclosing geolocation data without proof that people have agreed to that.[40]

Like the Court in *Carpenter,* the proposed order recognizes that not all government uses of geolocation data are alike.[41] It has exceptions for the disclosure of geolocation data for certain bona fide national security and data security purposes, including countering espionage and disrupting cyber threats from foreign ''nation states, terrorists, or their agents or proxies.'' [42] It also has exceptions for Federal law enforcement agencies responding ''to an imminent risk of death or serious bodily harm to a person.'' [43]

Unless one of these special exceptions applies, agencies like DHS, DEA, FBI, and IRS will not be able to use Venntel to warrantlessly track people to church, to the doctor, to school, to protests, or to their homes. And Venntel will soon not be able to trade in any geolocation data without the consent of the people being tracked.

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

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. The Alleged Harms From Respondents' Conduct

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

[32] *See Carpenter,* 585 U.S. at 311 (*citing United States* v. *Jones,* 565 U.S. 400, 415 (2011) (Sotomayor, J., concurring)). Furthermore, while it may be easier to refrain from using an app than to stop using a smartphone altogether, the complaint makes clear that the customers whose geolocation information has been collected by Venntel have in no way voluntarily ''assume[d] the risk'' of disclosing their geolocation information in this manner. *See id.* at 315; Complaint, *supra* note 10, at 5–9. In sum, it is easy to agree with my colleague Commissioner Holyoak, who wrote that our enforcement actions protecting precise geolocation ''[correlate] with judicial recognition, in other contexts, of how significant such information is.'' *See* Concurring Statement of Comm'r Melissa Holyoak, Kochava, Inc., FTC Matter No. X230009, at 2 (July 15, 2024) (''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.*

[33] 18 U.S.C. 2510 through 2522.

[34] 18 U.S.C. 2703(d).

[35] *Id.* 2710(b)(2)(C). Separately, while it cannot yet constitute ''an established public policy,'' I would be remiss if I did not note that The Fourth Amendment Is Not For Sale Act, which would extend these Fourth Amendment protections to geolocation data held by data brokers, recently passed the House of Representatives. *See* H.R. 4639, 118th Cong. (2023).

[36] 47 U.S.C. 551(c).

[37] *See* Order, Gravy Analytics, Inc. & Venntel, Inc., FTC Docket No. 2123035 at 5 (''II. Prohibitions on the Use, Sale, or Disclosure of Sensitive Location Data'').

[38] *See id.* at 4–5.

[39] *See id.* at 7–8 (''IV. Other Location Data Obligations'').

[40] *See id.* at 9 (''VI. Limitations on Collection, Use, Maintenance, and Disclosure of Location Data''). These are just a few parts of the order, which includes various other provisions and exceptions.

[41] *See Carpenter,* 585 U.S. at 319.

[42] Order, *supra* note 37.

[43] *See id.* at 4. These should not be understood as ''exceptions'' to section 5, but rather a recognition that in this specific instance, these order provisions are appropriate.

[1] Compl. ¶¶ 76–81.

[2] *Id.* ¶¶ 7–9.

[3] *Id.* ¶ 9.

[4] *Id.* ¶¶ 7, 13–22.

conditions derived from insights about their geolocation data.[5]

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 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. The Proposed Order and Count III of the Complaint

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 questions about the necessity and efficacy of the injunctive provisions found in Sections VI, VII, and IX,[18]

---

[5] *Id.* ¶¶ 44–45, 50–53.

[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 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, Public Law 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.*

[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

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]

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 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''

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.

[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.

[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.*

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.

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 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]

[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.

[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.

[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

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 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

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.

[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.*

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