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

Office of Commissioner
Andrew N. Ferguson

Concurring and Dissenting Statement of Commissioner Andrew N. Ferguson
In re Gravy Analytics, Inc. & In re Mobilewalla, Inc.
Matter Numbers 2123035 & 2023196

December 3, 2024

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]

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

[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).

directly to him, the sale of the data happens entirely without his knowledge.[11] Finally, given that the anonymized data remain valuable to firms for advertising and analytics, the injury that the consumer suffers is not outweighed by any countervailing benefits for the consumer.[12] The sale of non-anonymized, precise location data without first obtaining the meaningfully informed consent of the consumer is therefore an unfair act or practice in violation of Section 5.

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

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

---

[11] 15 U.S.C. § 45(n).
[12] *Ibid*.
[13] Gravy Complaint ¶¶ 76–78; Mobilewalla Complaint ¶¶ 71–72.
[14] Section 5 does not impose strict liability for the purchase of precise location data collected without the consumer's consent, nor do I understand the complaints and orders as interpreting Section 5 hold data brokers strictly liable for every purchase of precise location data that was collected without the consumer's consent. Data brokers need only take reasonable steps to ensure that the data they are acquiring were originally collected with the consumer's consent. Gravy Complaint ¶ 76 (faulting Gravy for not taking "reasonable steps to verify that consumers provide informed consent to Respondents' collection, use, or sale of the data for commercial and government purposes."); Mobilewalla Complaint ¶ 71 (similar).
[15] Mobilewalla Complaint ¶ 70.
[16] *Id.* ¶ 9.
[17] *Ibid*.
[18] *Id.* ¶¶ 12–15.
[19] *Id.* ¶ 18.
[20] Mobilewalla Complaint ¶ 10.

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]

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

[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.

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

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

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

We can already see this dysfunction in these complaints, which mention as sensitive characteristics race, ethnicity, gender, gender identity, sexual orientation, pregnancy, parenthood, health conditions, religion, and attendance of a political protest, among others.[27] While some of these characteristics often entail private facts, others are not usually considered private information. Attending a political protest, for example, is a public act. The public expression of dissatisfaction or support is the point of a protest. Treating attendance at a political protest as uniquely private and sensitive is an oxymoron. Moreover, there are no objective criteria on which to base this list.[28] The statute provides no guidance. The list is therefore a purely subjective creation of Commission bureaucrats. And it excludes categories that many would consider deeply

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

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

[27] Mobilewalla Complaint ¶¶ 27–32.

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

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

[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.

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.