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

Office of Commissioner
Alvaro M. Bedoya

**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***

**In the Matter of Gravy Analytics, Inc. & Venntel, Inc.**

**December 2, 2024**

I.

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

---

[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).

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]

II.

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?

---

[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.

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.

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

---

[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.

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

---

[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.

*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 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.

---

[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.

[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. §§ 2510–22.

[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).

IV.

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 protests, 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.

---

[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.