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

Office of Commissioner
Melissa Holyoak

Concurring Statement of Commissioner Melissa Holyoak

Kochava Inc., FTC Matter No. X230009

July 15, 2024

I vote to support the Commission's amended complaint against data broker Kochava and its wholly-owned subsidiary Collective Data Solutions, LLC ("CDS") (collectively "Defendants"), which the Commission alleges sell invasive profiles about consumers as well as precise mobile location data that identifies consumers' visits to sensitive locations. According to the complaint, the data the Defendants sell is sufficiently detailed and identifiable to reveal individuals' location at, and participation in, particular political, medical, or religious activities.[1] I write separately to highlight the significance of the Commission's action to protect the privacy of consumers' precise geolocation information.

The procedural posture of this case is important. The Commission rarely litigates privacy matters and is in the middle of hard-fought litigation against Kochava.[2] In fact, the Commission recently won an important, albeit preliminary, victory. In February 2024, the district court for the District of Idaho denied Kochava's motion to dismiss in its entirety,[3] determining that the Commission had adequately pled, under Section 5 of the FTC Act, two theories of substantial injury to consumers: (1) "putting [consumers] at an increased risk of suffering secondary harms, such as stigma, discrimination, physical violence, and emotional distress," and (2) "invading their privacy."[4] Today, the Commission authorizes staff to amend the complaint to name CDS, to which Kochava appears to have transferred its data broker business, and to allege that Kochava and CDS operate a common enterprise.[5] These amendments are necessary for the Commission to continue to vigorously pursue this action against Defendants and secure appropriate relief.

---

[1] *See, e.g.*, Sec. Amend. Compl. ¶ 15 (alleging that Kochava's precise geolocation data "reveal[s] [consumers'] movements throughout a day, week, month, year, or even more, including their visits to sensitive locations—for example, locations associated with medical care [and, inter alia] . . . religious worship"); ¶ 71 (describing Kochava's claims that "its audience segments allow customers to '[f]ind devices that intersect with important events or locations, or seek out devices that spend time in areas targeted by your campaign' and '[u]understand voter visitation to home, work, places of business, government buildings, and more'"); ¶ 96 (describing a Kochava customer's use of Kochava's data to identify "'Likely Republican Voter' . . . based on consumers' visits to 'Republican focused political events and events and venues affiliated with conservative topics.'").

[2] The Commission first filed its complaint against Kochava in federal court in 2022, followed by an amended complaint in June 2023. *FTC v. Kochava, Inc.*, FTC Cases and Proceedings, last updated Feb. 5, 2024, https://www.ftc.gov/legal-library/browse/cases-proceedings/ftc-v-kochava-inc.

[3] *FTC v. Kochava Inc.*, No. 2:22-cv-00377, 2024 WL 449363 (D. Idaho Feb. 3, 2024).

[4] *Id.* at *4-5.

[5] Sec. Amend. Compl. ¶¶ 6, 12.

The district court's decision in *Kochava* is an important marker in how to consider "substantial injury" in the context of privacy actions brought under Section 5. The opinion is significant, in part, because the vast majority of the Commission's privacy and data security matters have been settlements, not litigated actions. Sometimes that has been for good reason. Litigation is time-consuming and expensive. Prior Commissions have made thoughtful decisions to obtain settlements that leave consumers better off[6]—making difficult choices aimed at preserving the Commission's resources to pursue more matters in the public interest. But as courts continue to take a close look at the actions and presumed authorities of federal agencies,[7] it remains critical that we account for judicial analysis. Any future court decision in this litigation will be another important marker for the Commission to consider.

But even if this were an initial complaint, rather than a second amendment, I would support this matter because 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. For example, in *Carpenter v. United States*,[8] the Supreme Court addressed how wireless companies had "detailed, encyclopedic, and effortlessly compiled" cell phone location information,[9] which "provides an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations."[10] The Court equated tracking a cell phone to "attach[ing] an ankle monitor to the phone's user."[11]

At the Commission, we consider location privacy in the context of Section 5, not the Fourth Amendment to the Constitution. And this complaint focuses on sales of precise geolocation data and related sensitive information to commercial purchasers, not law enforcement. But the *Carpenter* Court's description of the sensitivity of precise geolocation data is instructive here, especially given how government officials can purchase precise geolocation data from commercial

---

[6] Statement of Chairman Joe Simons and Commissioners Noah Joshua Phillips and Christine S. Wilson, *In re Facebook, Inc.*, at 1 (July 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536946/092_3184_facebook_majority_statement_7-24-19.pdf ("The record-breaking penalty and unprecedented, sweeping conduct relief [in a consent order] . . . far exceeds what the Commission could expect to receive at the end of litigation years from now."); *id.* at 6 (explaining "[l]itigation would have delayed the imposition of these important consumer protections . . .").

[7] *Cf. Loper Bright Enters. v. Raimondo*, 144 S. Ct. 2244 (2024) (ending "*Chevron* deference" to federal agencies); *SEC v. Jarkesy*, 144 S. Ct. 2117 (2024) (holding that the Seventh Amendment entitles the defendants to a jury trial when a federal agency seeks civil penalties); *AMG Capital Mgmt., LLC v. FTC*, 593 U.S. 67 (2021) (holding that Section 13(b) of the FTC Act does not authorize the Commission to seek, or a court to award, equitable monetary relief).

[8] 585 U.S. 296 (2018).

[9] *Id.* at 309.

[10] *Id.* at 311 (cleaned up).

[11] *Id.* at 312; *cf. United States v. Jones*, 565 U.S. 400, 430 (2012) (differentiating between the government's "relatively short-term monitoring of a person's movements on public streets [that] accords with expectations of privacy that our society has recognized as reasonable" with "longer term GPS monitoring in investigations of most offenses [that] impinges on expectations of privacy") (Alito, J., concurring).

data brokers in ways that may circumvent Fourth Amendment protections.[12] There 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.[13] For consumers to realize the benefits of technology, they must be able to trust that technology—including tools that hold their sensitive personal data—will remain secure from wrongful government surveillance.[14] When private parties like the Defendants disclose precise geolocation information revealing political, medical, or religious activities, without consumers' consent to willing purchasers, their conduct breaches that trust and jeopardizes Americans' freedoms.

---

[12] *See, e.g.*, 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-media-cellphone-dataminr-venntel/. Several dissenting justices in *Carpenter* criticized the majority's departure from precedent that "individuals have no Fourth Amendment interests in business records which are possessed, owned, and controlled by a third party." 585 U.S. at 321 (Kennedy, J., dissenting). But as Justice Gorsuch explained, we do everything on the internet with our most private information residing on third party servers: "[Precedent] teach[es] that the police can review all of this material, on the theory that no one reasonably expects any of it will be kept private. But no one believes that, if they ever did." 585 U.S. at 387 (Gorsuch, J., dissenting). Justice Gorsuch further observed: "Just because you entrust your data—in some cases, your modern-day papers and effects—to a third party may not mean you lose any Fourth Amendment interest in its contents." *Id.* at 400.

[13] *See, e.g.*, *Financial Surveillance in the United States: How Federal Law Enforcement Commandeered Financial Institutions to Spy on Americans*, Interim Staff Report, Committee on the Judiciary and Select Subcommittee on the Weaponization of the Federal Government, U.S. House of Representatives, at 1 (Mar. 6, 2024) (explaining how "Bank of America (BoA), voluntarily and without legal process, provided the FBI with a list of names of all individuals who used a BoA credit or debit card in the Washington, D.C. region between the dates of January 5 and January 7, 2021. Mr. Hill also testified that this BoA 'data dump' of customer information also included a list of individuals who had ever used a BoA credit or debit card to purchase a firearm, regardless of when or where it was purchased." (citations omitted)), https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/How-Federal-Law-Enforcement-Commandeered-Financial-Institutions-to-Spy.pdf; *see id.* at 8 ("The emergence of credit cards, mobile banking, and other digital marketplaces have resulted in an unprecedented amount of private data entrusted to financial institutions, potentially revealing all sorts of sensitive information about a customer. For that reason, financial records have become an important investigative tool for federal law enforcement. Still, federal law enforcement's interest in financial records must be weighed against the privacy interests of Americans. Without greater oversight and the necessary legislative reforms reflecting the advances in modern-day banking practices, Americans' private financial data is still vulnerable to the shortcomings of an outdated legal framework and pervasive government surveillance." (citations omitted)); *id.* (describing an "expansive, backdoor information-sharing regime led by the nation's most powerful law enforcement agencies and their partners in the financial sector").

[14] *See* Letter to Attorney General Merrick Garland and FBI Director Christopher Wray from Virginia Attorney General Jason Miyares and joined by 19 State Attorneys General (Feb. 10, 2023) (expressing outrage at FBI internal memorandum that targeted Catholics as potential threats due to their religious beliefs), *available at* https://attorneygeneral.utah.gov/wp-content/uploads/2023/02/Letter-to-Attorney-General-Garland-Director-Wray-2.10.2023-002-1.pdf.