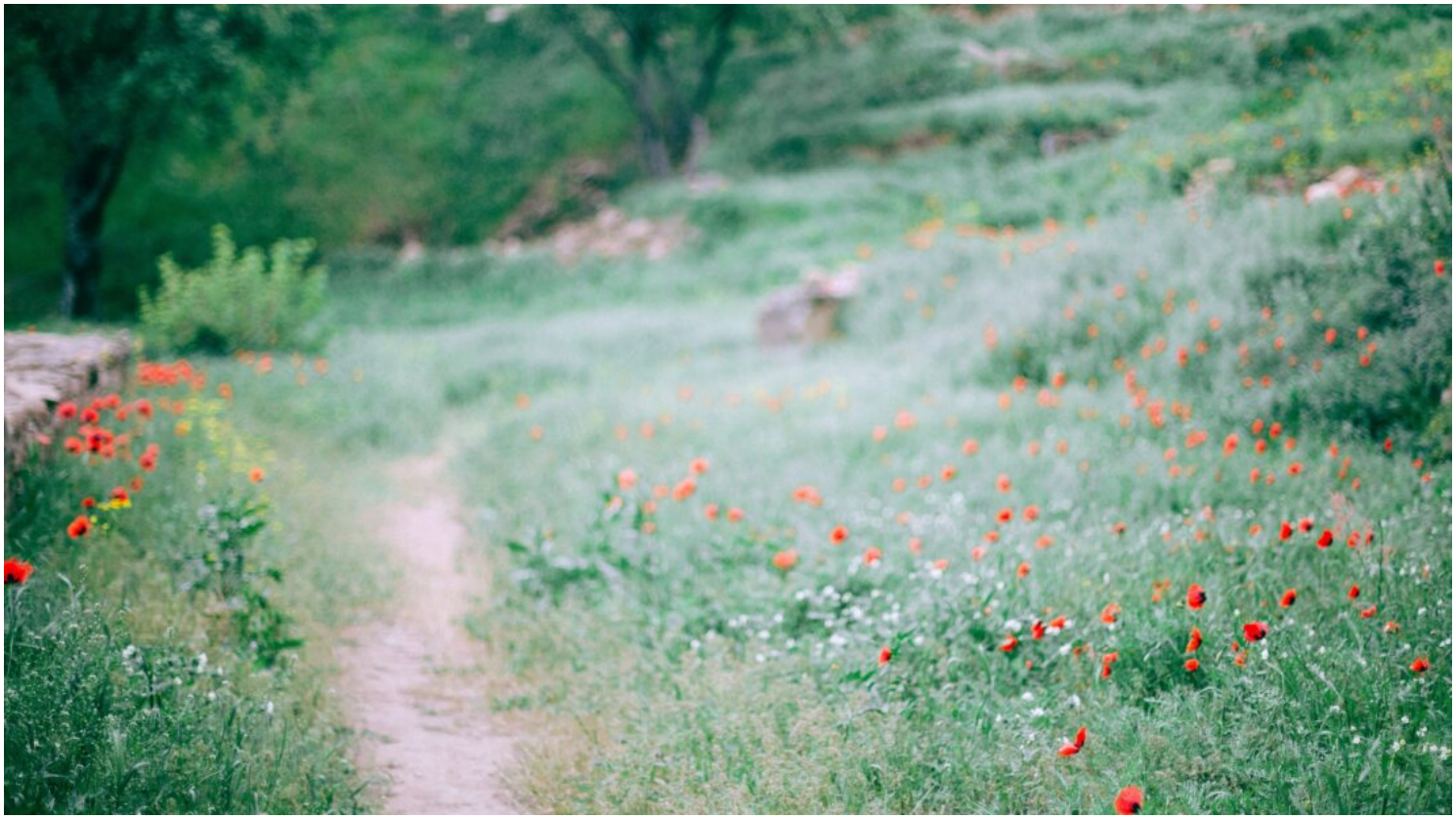
SQUIRE PATTON BOGGS

Privacy World

Keeping you informed on the evolving law on data privacy, security and innovation.

Sensitive Data Processing is in the FTC's Crosshairs



By Glenn A. Brown, Kristin Bryan, Kyle Dull & Alan Friel on February 9, 2024

As state legislation increasingly regulates sensitive data, and expands the concepts of what is sensitive, the Federal Trade Commission ("FTC" or "Commission") is honing-in on sensitive data

processing in expanding its unfairness authority in relation to privacy enforcement. The FTC's recent enforcement activities regarding location aware data is a good example. As we have previously reported **here** and **here**, Kochava, an Idaho-based data broker, is currently embroiled in a federal lawsuit with the Commission that has the potential to redefine the legal bounds of sensitive data collection, use and sharing and the data brokering industries on a federal level.

You may think, how is the FTC targeting data brokers when there is no omnibus federal privacy law for the FTC to enforce? Look no further than the unfairness doctrine under Section 5 of the Federal Trade Commission Act ("FTC Act"). The Kochava case centers on the question of whether Kochava's potentially unrestricted sale of precise consumer precise geolocation data constitutes an unfair business practice under the FTC Act. Notably, the Kochava complaint does not raise a deception allegation. The continued litigation follows the settlement of two enforcement actions also addressing allegedly unfair *and deceptive* location-aware data processing activities.

Key Takeaways

- Geolocation data paired with a persistent identifier, such as an advertising or device ID, even if not directly connected to a named individual consumer, is sensitive personal data according to the FTC. This should come as no surprise and reflects the approach taken by recent state privacy laws as well as the approach taken in Europe and other countries.
- Before a business can collect, sell, or share sensitive personal data (or at least precise location) the business must either:
    - Effectively provide the consumer with sufficient disclosures describing the categories of information collected, the purpose, the types of entities receiving the data, and a simple mechanism for consumers to opt-out or withdraw consent; *or*
    - Obtain the consumer's express, affirmative consent to the collection, sale, or sharing of sensitive personal information.
    - In either case, the FTC will apply its clear, conspicuous and proximate standards to the notices.
- Substantial injury ("likely to cause substantial injury") to consumers, a requirement to establish unfairness under Section 5, can be established by the mere risk that location data could be used to identify people and track them to sensitive locations (e.g., medical facilities, LGBTQ+ associated locations, etc.), because that may expose consumers to secondary harms (e.g., stigma, discrimination, physical violence, emotional distress, etc.) or it may be an invasion of the consumer's privacy. This standard has now survived a motion to dismiss

challenge in federal court and is the standard currently used under the FTC's recent consent orders regarding other location data brokers.

- While recent enforcement actions have been brought against companies that leverage another business' direct relationship with the consumer to collect sensitive data (e.g., mobile app publishers), business that use, or allow others to use, tracking technologies to track consumers should consider providing consumers with enhanced disclosures (e.g., explaining all of the uses and types of recipients of location data where location services are activated) regarding the use of such tracking technologies and how opt-out of the tracking, especially if sensitive information is involved.
- By choosing to litigate Kochava solely based on an unfairness claim (and not deception) the FTC has the potential for establishing judicial precedent that privacy harms are cognizable and significant and can outweigh any benefits to competition or consumers, greatly expanding the FTC's authority to regulate privacy matters.

The FTC's Toolkit to Address Privacy Concerns

Consumer tracking has been of interest to the FTC for some time now and the FTC has attempted to address the topic in different ways, including supporting proposed federal **Do Not Track legislation**, through its power to **prohibit deception**, and most recently unfairness claims. The current enforcement trend of using unfairness harkens back to the **FTC's Vizio settlement**, which resolved **allegations** that smart-TV manufacturer, Vizio, captured "sensitive" television viewing activity of consumers and shared this information with third parties to target advertising without the consumer's consent. Collecting and sharing such data, without the consumer's consent, was deemed to have caused substantial injury to the consumers, and this injury was sufficient to warrant a finding of unfairness, at least according to the FTC. During the Trump-era, unfairness took a back seat to deception in privacy protection efforts by the Commission. That is not the case under Chairperson Kahn's FTC.

Whether a practice is unfair depends on three criteria: (1) whether the practice, without necessarily having been previously considered unlawful, offends public policy as it has been established by statutes, the common law, or otherwise-whether, in other words, it is within at least the penumbra of some common- law, statutory, or other established concept of unfairness; (2) whether it is immoral, unethical, oppressive, or unscrupulous; and (3) whether it causes substantial injury to consumers (or competitors or other businesses). The injury: (1) "must be substantial;" (2) "it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces;" and (3) "it must be an injury that consumers themselves could not reasonably have avoided." ***FTC Policy Statement on Unfairness***. This balancing test was added by Congress in the

early 1980's to temper the FTC's unfairness authority, specifically in response to potential bans or restrictions on children's advertising – an issue that is also seeing a resurgence. As privacy harms are becoming more recognized in the U.S., as reflected by the growing number of U.S. privacy laws, unfairness is starting to be a more viable tool for the FTC to use to restrict what it refers to as "surveillance capitalism."

The FTC's Kochava Complaint and Amended Complaint

In August 2022, the FTC filed a Complaint seeking a permanent injunction against Kochava in the District of Idaho. Kochava subsequently filed a motion to dismiss. In May 2023, the District Court dismissed the FTC's Complaint, ruling that the allegations, even if proven true, were not sufficient to show that Kochava's data alleged practices created a "significant risk" of harm to consumers. However, the FTC was allowed to amend and refile its Complaint.

The FTC filed an **Amended Complaint in June 2023** that included more specific allegations. The Amended Complaint alleged that in many cases Kochava "provides data that directly links … precise geolocation data to identifying information about individual consumers, such as names, addresses, email addresses, and phone numbers." According to the FTC's Amended Complaint, Kochava's marketing materials promoted its ability "to connect each individual consumer to multiple 'data points' in order to ensure that its customers are able to continuously track consumers and connect consumers' activities with historic and new data." The Amended Complaint also alleged that Kochava "directly links" precise geolocation data (timestamped latitude and longitude coordinates) with a persistent Mobile Advertising ID that "is assigned by a mobile device's operating system to allow companies to track a consumer's mobile activity and is used to send targeted advertisements."

Kochava's Motion to Dismiss is Denied

Kochava promptly filed a motion to dismiss the FTC's Amended Complaint, arguing that the deficiencies in the original Complaint had not been cured. However, last week the District Court **denied** Kochava's motion to dismiss, finding that the FTC's more robust Complaint "is legally and factually plausible."

In denying the motion to dismiss, the Court notes that the FTC alleged "that the targeting of consumers based on geolocation data 'has and does occur.'" The FTC's allegations were "real-world examples of harms inflicted on device users due to the disclosure of their geolocation and app-use data," but notably, none of these examples involved Kochava's data. The real-world examples involving non-Kochava data were sufficient to support the FTC's claim under Section 5(n),

according to the District Court, because the FTC only needed to "allege that Kochava's acts or practices cause *or are likely to cause* substantial injury to consumers."

The Court also supported the FTC's theory that substantial injury can be inflicted "on consumers by invading their privacy." In doing so, the District Court pointed to decisions from the United States Supreme Court and the Ninth Circuit Court of Appeals that found that certain modern technologies can result in unreasonable intrusions to privacy rights. *See Carpenter v. United States*, 138 S.Ct. 2206, 2217 (2018); *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1272 (9th Cir. 2019); *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020) (holding that compiling "highly personalized profiles from sensitive browsing histories and habits" could be a "highly offensive" invasion of privacy). Kochava, according to the FTC, sells comprehensive, "raw and synthesized data designed to give its customers a '360-degree perspective' on the unique traits of millions of individual device users." This allegation is enough to support an invasion of privacy claim, and thus a substantial injury to consumers, because it "is substantial both in quantity and quality."

Now that the District Court has ruled that the case may proceed, it will be interesting to see whether Kochava will settle with the FTC or litigate the issues. Kochava appears to fundamentally disagree with many of the FTC's characterization of the practices at issue in the Amended Complaint, which appears to have previously motivated efforts by the company to have filings in this litigation sealed. That effort was ultimately unsuccessful as in November 2023, the District Court granted the FTC's motion to unseal the Amended Complaint (and simultaneously denied Kochava's motion for sanctions against the FTC under Rule 11). In doing so, the court found no "compelling reason" to keep the FTC's Amended Complaint under seal. The Court rejected Kochava's arguments that the allegations in the Amended Complaint are "knowingly false" because they "intentionally conflate separate and distinct services offered by Kochava." This disagreement over the FTC's characterization of Kochava's practices will undoubtably continue as the case enters discovery—which will close on January 15, 2025.

Continued Federal Interest in Data Privacy Beyond Kochava

The Kochava case not only aligns with the FTC's increasing interest in data privacy beyond cybersecurity, but also serves to further recent federal policy initiatives. One initiative to note is the Biden Administration's executive order addressing security concerns over the disclosure of sensitive health-related data. This federal policy at first seems entirely disconnected from Kochava, which is not an app focused exclusively on health. But, as the FTC explains in its Complaint, Kochava's brokerage of "precise geolocation data" makes it possible to track consumers to

sensitive locations such as "places of religious worship … domestic abuse shelters," and "medical facilities, and … women's reproductive health clinics."

The core claims and allegations in the Kochava complaint are congruent with recent efforts (at the federal level and otherwise) to more closely regulate the activities of data brokers, particularly when it comes to the handling of sensitive information. This increased focus is anticipated to persistent well into 2024 and beyond. More broadly, the FTC's Amended Complaint against Kochava also reflects the agency's broad interpretation of what constitutes "unfair" acts and practices under Section 5 to encompass issues bearing upon consumer privacy—which will impact entities across industries in the months to come.

Kochava is not the only location-aware data broker that has been targeted by the FTC. Just last month, the **FTC issued orders prohibiting data brokers, X-Mode Social, Inc. and Outlogic, LLC**, from sharing or selling sensitive personal information such as precise geolocation data, which is the same type of sensitive personal information at issue in Kochava, because such practices were unfair and failing disclose the use of location data was deceptive (note the deception claim here that is missing in Kochava). X-Mode/Outlogic represents the FTC's first settlement with a data broker concerning the collection, sale, and sharing of sensitive location information.

A few days later, the FTC also reached a **settlement with InMarket** resolving similar allegations regarding the collection, sale, and sharing of geolocation data. InMarket collects consumer geolocation data through its software development kit ("SDK") offered to third party apps (X-Mode/Outlogic also used an SDK to collect location information), as well as purchasing consumer information through other sources. InMarket then uses this data (including location data) to target advertising to consumers. According to the FTC, InMarket does not provide sufficient disclosures to consumers regarding its use of location data and does not provide third party app developers who use the SDK with sufficient information that would allow the third-party app developers to provide their own informed notice to consumers regarding the use of location data. InMarket's data practices were alleged to be both unfair and deceptive, similar to the allegations in X-Mode/Outlogic. In settling this matter, InMarket agreed to an SDK Assessment Program, among other obligations, that requires it to audit third party location data suppliers (i.e., third party apps using the InMarket SDK) to (1) confirm that consumers provide Affirmative Express Consent (a defined term), or (2) confirm that consumers specifically consent to the collection, use, and sale of their location data. Affirmative Express Consent means, among other things, the disclosure of "1) the categories of Covered Information that will be collected; (2) the purpose(s) for which the Covered Information is being collected, used, or disclosed; (3) a simple, descriptive URL (or hyperlink if technically possible) to a document that describes the types of entities collecting the Covered Information or to whom the Covered Information is disclosed; and (4) a simple,

descriptive URL (or hyperlink if technically possible) to a simple, easily located means by which the consumer can withdraw consent and that describes any limitations on the consumer's ability to withdraw consent." Complying with the Affirmative Express Consent requirement (prong 1 of the SDK Assessment Program) requires third party businesses to provide detailed disclosures to consumers, but this may be a preferrable alternative to explicitly obtaining specific consent to the sale of location data (prong 2 of the SDK Assessment Program).

While these requirements may be, in part, the "fencing in" of a prior offender, they are at minimum an expression of best practices that would pass FTC muster. Is this the FTC recognizing that some state consumer privacy laws require an affirmative opt-in to the collection and sale of sensitive personal data (e.g. Colorado and Viginia), while others provide for an opt-out (e.g., California)? Perhaps, but in either event the FTC's standard of clear, conspicuous and proximate pre-collection notice apply.

It's not only the Feds…State Regulation is Here

The FTC is not alone in expanding consumer privacy rights and increasing focus on data broker practices. Consumer privacy has been a hot topic for the last few years, with **more than a dozen states passing comprehensive consumer privacy laws, and several other states are considering similar laws**. In general, these state consumer privacy laws have notice obligations, and as noted above, approach sensitive personal data in different ways. A few states have laws regulating data brokers and requiring data brokers to register with the state. California also requires the California Privacy Protection Agency to set up a deletion mechanism that allows consumers to make requests to all registered data brokers, by January 1, 2026. We cover the data broker developments in California in more detail **here**. There is also legislation recently passed, or under consideration, in multiple sates that provides or proposes heightened standards for sensitive information, including biometrics, minor's personal data and online activities, religious or philosophical belief, union membership status, health-related data, sexual orientation and gender identity, and employee and public monitoring. Many of these state laws now or will soon require conducting, documenting, and in some cases filing with regulators, assessments of high-risk data processing activities, specifically including, without limitation, the processing of sensitive information. For more information on these requirement see our explainer **here**.

As the regulatory guardrails for data privacy evolve, we will be there to keep you appraised of the developments. For more information contact the authors or you SPB relationship partner.

Disclaimer: While every effort has been made to ensure that the information contained in this article is accurate, neither its authors nor Squire Patton Boggs accepts responsibility for any errors or omissions.

The content of this article is for general information only, and is not intended to constitute or be relied upon as legal advice.