WILSON
SONSINI

FTC Workshop

Overview of the FTC's Authority

Primary Statue: Section 5 of the FTC Act (15 USC 45)
Prohibits "unfair or deceptive acts or practices in or affecting commerce"

- Deception
  - Material misrepresentation
  - Likely to mislead a consumer acting reasonably under the circumstances
- Unfairness
  - Caused or is likely to cause substantial injury to consumers
  - Consumers could not reasonably avoid the injury
  - Not outweighed by countervailing benefits to consumers or competition
- Equitable monetary relief

Other Laws: Enforcement or administrative responsibility under more than 70 laws, including: COPPA (children's online privacy), FCRA (fair credit reporting), GLBA (financial privacy), ROSCA (fairness in subscription services)

- Monetary relief may include civil penalties

Data Brokers

Kochava: A federal district court denied Kochava's motion to dismiss the FTC's amended complaint, noting that the FTC has stated a plausible claim under Section 5 of the FTC Act.

X-Mode and InMarket: Settled actions with the FTC

- Companies can't use, sell, transfer, disclose US location data associated with "Sensitive Locations" (e.g., health-related locations, religious locations, prisons/jails, labor union offices, children's education/childcare locations, locations associated with ethnicity or race, shelter or social service locations)
- For the Location Data companies can collect, use, etc. they need to ensure the consumer provided Affirmative Express Consent (AEC) "if feasible." If the company receives Location Data from other parties, it needs to assess its suppliers to be sure consumers provided AEC or specifically consented to the collection, use, and sale of their Location Data.
- Location data collected without AEC, and any data products made using that location need to be deleted (i.e., algorithmic disgorgement)
- Consumers can withdraw consent and ask for data deletion, and companies have certain obligations to help them in exercising these rights (e.g., by providing a list of entities to whom their data has been disclosed or by passing along the consumer's deletion request to those entities).
- Note that these enforcement actions align with a broader Administration push to tamp down data broker transactions involving sensitive personal information and location data, especially international transactions

Health Data

- Changes to the **Health Breach Notification Rule (HBNR)**
- **U.S. v. Monument, Inc.**
- **U.S. v. Cerebral, Inc.**

Children

- **Tiktok**
  - FTC Investigation Leads to Lawsuit Against TikTok and ByteDance
- FTC COPPA Amicus Brief
- **FTC v. NGL Labs, LLC**
- **The Attention Economy: Monopolizing Kids' Time Online**

Cybersecurity

- FTC action against **Marriott and Starwood**
- **U.S. v. Vercada, Inc.**
- **Blackbaud** FTC order

Artificial Intelligence – Operation AI Comply

- **Operation AI Comply**
  - The FTC is taking action against the following companies for using AI to facilitate deceptive or unfair conduct:
    - DoNotPay
    - Ascend Ecom
    - Ecommerce Empire Builders
    - Rytr
    - FBA Machine

- FTC orders seeking information of surveillance pricing

- **U.S. Artificial Intelligence & Sustainability Summit**

- The FTC's FCC comment

- Changes to AI terms of service

SMVSS Report

The September FTC staff report found that major social media and video streaming companies engaged in vast user surveillance. More specifically, the report found that:

- Companies engaged in extensive consume surveillance to monetize their personal information while failing to adequately protect users online, especially children.
- Companies collected and could indefinitely retain data, including information from data brokers, and about both users and non-users of their platforms.
- Many of the companies' business models incentivised mass collection of user data to monetize, especially via targeted advertising, which accounts for most of their revenue.
    - These incentives were often at odds with the protection of user privacy.

Ultimately, the report recommends that these companies limit data retention and sharing, restrict targeted advertising, and strengthen protection for children and teens.

Dark Patterns

The International Consumer Protection and Enforcement Network (ICPEN) released an annual review detailing the use of dark patterns by websites and mobile applications

FTC Testimony Before Subcommittee

FTC Chair Lina M. Khan's testimony before the **Subcommittee on Innovation, Data and Commerce** outlined the FTC's work to protect privacy and data security.

Consumer Tracking

- ***FTC Avast Order***
- Hashing and data anonymity

The FTC in Context

- ***FTC and federal agencies, i.e., the CFPB***
- ***Congress – legislation and oversight***
- ***Interplay with the states – e.g., California***