

October 24, 2024

# Handle with Care: Browsing and Location Data

**Bhavna Changrani**  
Federal Trade Commission

**Adonne Washington**  
Future of Privacy Forum

**Steve Wernikoff**  
Honigman LLP



## **Bhavna Chagrani**

Attorney, Division of Privacy and  
Identity Protection  
Federal Trade Commission



## **Adonne Washington**

Policy Counsel for Data, Mobility, Location  
Future of Privacy Forum



## **Steve Wernikoff**

Partner  
Honigman, LLP

**“Browsing and location data  
are sensitive. Full stop.”**

[FTC Technology Blog, March 4, 2024](#)

# Location Data

“[I]ndividualized geolocation data is sensitive and merits heightened consent methods.”

Affirmative express consent except fulfillment, fraud prevention, internal operations, legal compliance.



## Protecting Consumer Privacy in an Era of Rapid Change

RECOMMENDATIONS FOR  
BUSINESSES AND POLICYMAKERS

FTC REPORT

# Location Data

“Among the most sensitive categories of data collected by connected devices [is] a person’s precise location[.] . . . [L]ocation data can reveal a lot about people, including where we work, sleep, socialize, worship, and seek medical treatment.”

- FTC Acting Associate Director, Division of Privacy & Identity Protection, July 11, 2022

## FTC settles unprecedented case against geolocation data broker

## FTC settles second case with geolocation data broker in two weeks

The Record.  
Recorded Future News

# FTC alleges data broker exposes users to violent threats by selling location data

**THE HILL**

BY REBECCA KLAR - 08/29/22 12:08 PM ET



## Themes of FTC Claims

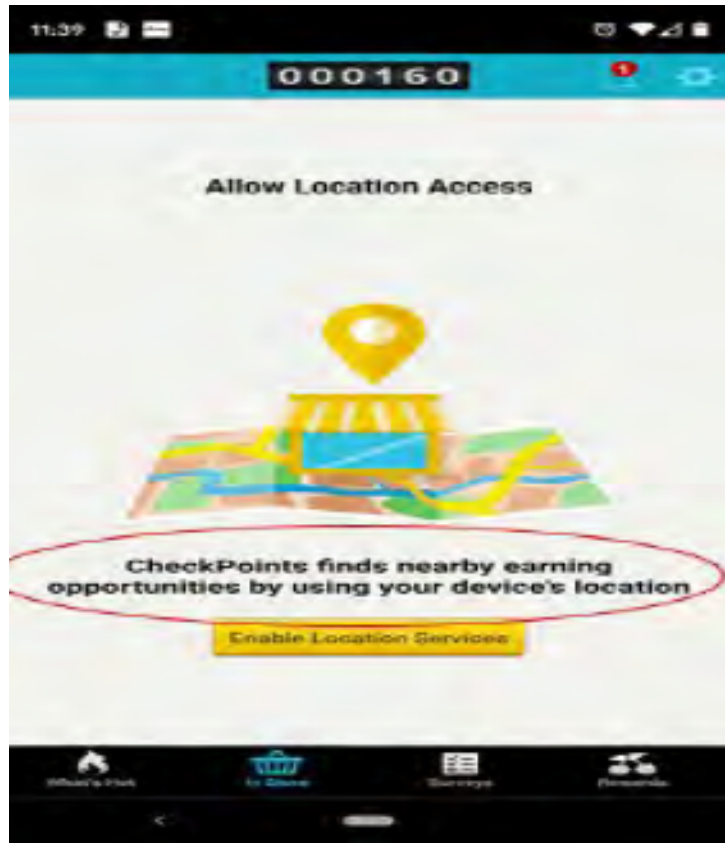
- Unfair collection, use and sale of sensitive data
- Unfair failure to honor consumer privacy choices
- Unfair categorization of consumers for marketing purposes
- Unfair retention of location data
- Deceptive failure to disclose use of location data

## FTC Settlement Terms

- Prohibitions on misrepresentations
- Consent to Collect, Use, Maintain & Disclose Location Data
- Prohibition on Selling Location Data
- Sensitive Location Data Program
- Supplier Assessment Program
- Data Retention Limits
- Honoring Deletion Requests
- Mandated Privacy Program

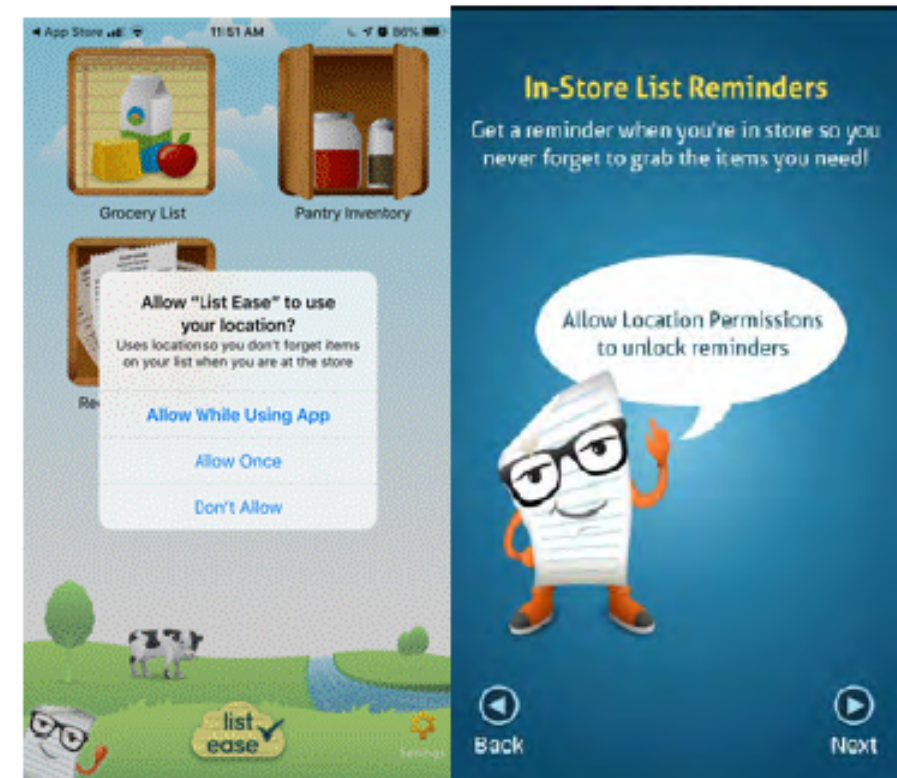


## What is Proper Consent?



Half-truths are untruths.

Vaguely worded disclosures don't give a company free license to use or sell people's sensitive location data.



## What is Proper Consent?

“Consent” to one use without an explanation of other uses is not consent at all.

### Consent Notice

We hope you are enjoying Drunk Mode! We really appreciate your support. To fund our operation costs and development of new features, we collect and share mobile ad IDs and location data with third parties to help them conduct ad personalization and location-based analytics including ad performance, market research, and traffic and health research. By proceeding you agree to the processing of personal data as described in our partners privacy notices. You can go to your device settings at any time to withdraw (or deny) your consent.

ACCEPT

PRIVACY POLICY

## Deletion Requests & Deidentification

Respondent must delete or Deidentify historic location data

“**Deidentify**” means information that cannot reasonably identify, be associated with, or be linked, directly or indirectly, to a particular consumer, provided that Respondent:

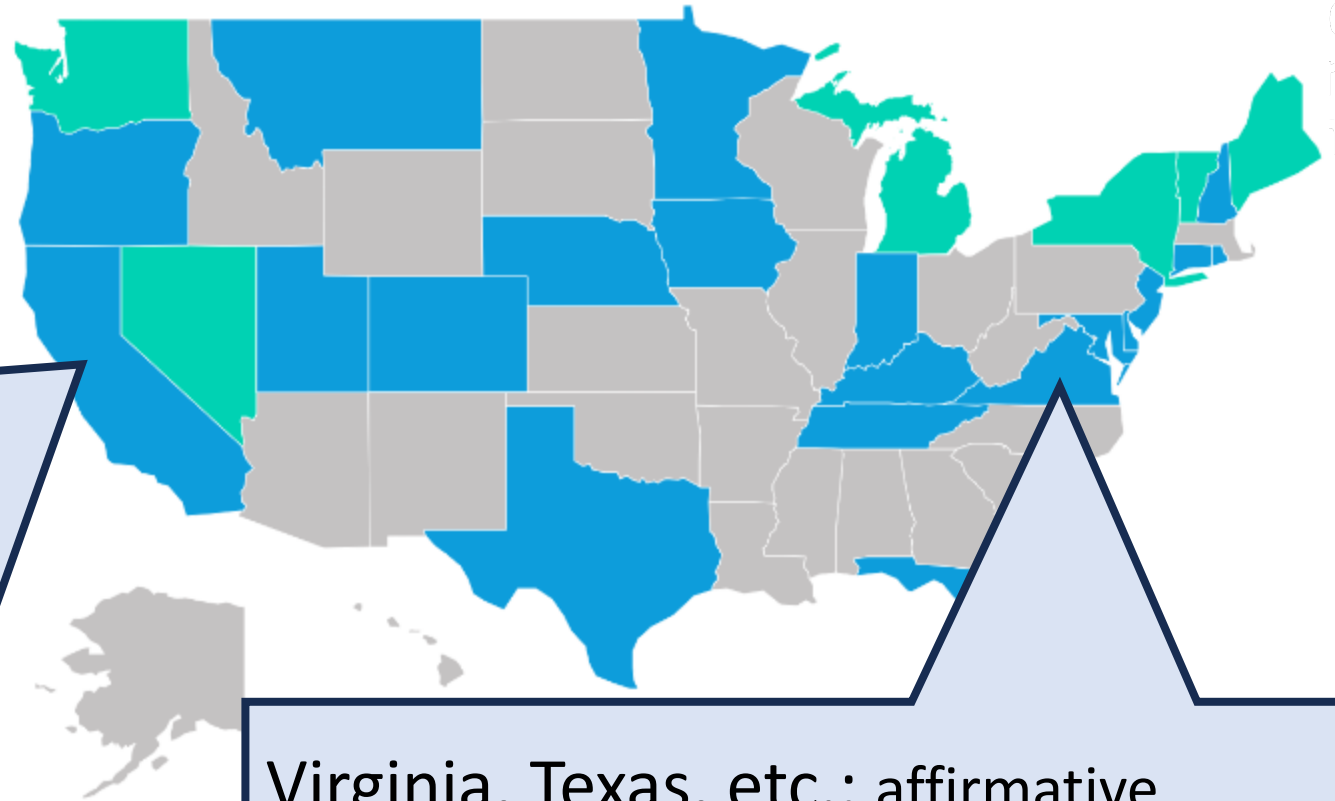
- Has implemented technical safeguards to prohibit reidentification
- Has implemented business processes that prohibit reidentification
- Has implemented business processes to prevent inadvertent release of deidentified data
- Makes no attempt to reidentify the information

Data that is linked to a mobile advertising ID or an individual’s home is not Deidentified.

# Location Data

## California:

- **Defined:** Data used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet
- **“Right to Limit”** use and disclosure of sensitive data to what is necessary to perform the services or provide the goods reasonably expected by an average consumer



Virginia, Texas, etc.: affirmative consent to process subject to exceptions, including: legal compliance, comply with LE, defend legal claims, provide product or service, safety, fraud detection, internal research

**“Location Data”** means any data that reveals a mobile device’s or consumer’s precise location . . . or any unique persistent identifier combined with such data, such as a mobile advertising identifier or identifier for advertisers. Data that reveals only a mobile device or consumer’s coarse location (e.g., zip code or census block location with a radius of at least 1,850 feet), or that is used solely for the purpose of generating such coarse location and then deleted within 48 hours of collection, is not Location Data.

# Browsing Data

“A person’s browsing history can reveal extraordinarily sensitive information. A record of the websites someone visits can divulge everything from someone’s romantic interests, financial struggles, and unpopular political views to their weight-loss efforts, job rejections, and gambling addiction.”

- Statement of FTC Chair Lina Khan, Feb. 21, 2024

# Browsing Data

**UNITED STATES OF AMERICA  
BEFORE THE FEDERAL TRADE COMMISSION**

**COMMISSIONERS:**

**Lina M. Khan, Chair  
Rebecca Kelly Slaughter  
Alvaro M. Bedoya**

**In the Matter of**

**AVAST LIMITED, a United Kingdom limited liability company,**

**AVAST SOFTWARE S.R.O., a Czech Republic limited liability company, and**

**JUMPSHOT, INC., a Delaware company.**

**DOCKET NO.**

**COMPLAINT**

Alleged security software company collected browsing information through browser extensions and antivirus software installed on computers & mobile devices

Alleged company sold consumers' granular and re-identifiable browsing information through subsidiary

Alleged consumers were told software would protect privacy and any disclosure of browsing info would be in aggregate and anonymous form

## FTC Claims

- Unfair collection, retention and sale of browsing data
- Deceptive failure to disclose tracking of consumers
- Misrepresentations regarding aggregation & anonymization



## FTC Settlement Terms

- Prohibition on sale or disclosure of browsing data from any Avast Product, or derived from Avast Product to a Third Party for advertising
- Obtain consent for sale or disclosure of browsing data from non-Avast Products to a Third Party for advertising
- Prohibition on misrepresentations about processing of data
- Delete browsing data transferred to subsidiary
- Mandated privacy program
- Privacy program assessments by a third party
- \$16.5 million payment

“**Browsing Information**” means, in whole or in part, any uniform resource locators (URLs) of page requests, the URLs of background resources, search queries, form values, and the value of cookies placed on consumers’ computers by a Third Party corresponding to the consumers’ navigation of the World Wide Web collected from consumers or their devices.”

“**Third Party**” means an entity other than: (1) Respondents, (2) a service provider of Respondents that: (a) uses or receives [personal data] collected by or on behalf of Respondents for and at the direction of Respondents and no other individual or entity, (b) does not disclose the [personal data] or info derived from such data to an entity other than Respondents or a subcontractor to such service provider bound to contractual terms, and (c) does not use the data for any other purpose; or (3) any entity that uses [personal data] only as reasonably necessary: (a) to comply with applicable law, regulation, or legal process, (b) enforce Respondents’ terms, or (c) to detect, prevent, or mitigate fraud or security vulnerabilities.

**UNITED STATES OF AMERICA  
BEFORE THE FEDERAL TRADE COMMISSION**

**COMMISSIONERS:**

**Lina M. Khan, Chair  
Rebecca Kelly Slaughter  
Alvaro M. Bedoya**

**In the Matter of**

**AVAST LIMITED, a United Kingdom limited liability company,**

**AVAST SOFTWARE S.R.O., a Czech Republic limited liability company, and**

**JUMPSHOT, INC., a Delaware company.**

BC

“Re-identifiable browsing information is sensitive data”

**COMPLAINT**

## CIPA

Alleged aiding and abetting an unlawful interception of message content under Cal. Penal Code 631(a)(4)

UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA

M.G., Plaintiff, v. THERAPYMATCH, INC., Defendant.

Case No. 23-cv-04422-AMO

September 16, 2024, Filed

September 16, 2024, Decided

“While a URL that includes ‘basic identification and address information’ is not ‘content,’ a URL disclosing a ‘search term or similar communication made by the user’ could constitute a communication under the statute.”

“Similarly, log-in buttons and descriptive URLs are ‘contents’ within the meaning of the CIPA because they reveal the ‘path’ and ‘query string,’ i.e., that the user searched for a specific doctor and searched for information about diabetes.”

# Questions & Contacts



## **Bhavna Chagrani**

Attorney, Division of Privacy and  
Identity Protection  
Federal Trade Commission



## **Adonne Washington**

Policy Forum  
Counsel for Data, Mobility, Location  
Future of Privacy



## **Steve Wernikoff**

Partner  
Honigman, LLP