June 2024

Data Brokers

By Mark Costlow

This month we're looking into the shadowy world of data brokers. What are they collecting, how are they getting it, and why? After setting the stage, we'll dig deep into one particular kind of data that is very valuable to brokers: your location.

What are they?

Data brokers collect, process, and sell personal information about individuals. They gather data from both public and private sources. Their customers are businesses that can use the data to improve sales or further other goals. They include marketers, advertisers, and **government agencies, especially police departments**.

"Data Aggregation" is the collection of information from many sources and synthesizing it into detailed profiles of individuals. The profiles include personal information like names, addresses, phone numbers, purchase behaviors, and interests, as well as sensitive information like financial status or health data. This aggregation is the value the brokers add for their customers. All of those data points exist out there, and the brokers are the ones who suck it up and piece it together to make a picture of you the individual, identifying the ways you can be influenced or used for their gain.

Who are they?

Some data brokers you have probably heard of are the big three credit reporting agencies: Experian, Equifax, and TransUnion. They have all pivoted from simply providing credit reports to collecting and selling more detailed information about us. That includes consumer data like buying habits and preferences, and even "**Predictive Analytics**" to predict future consumer behavior.

Other players are companies you probably have not heard of like X-Mode and Fog Data Science, who both specialize in location data. Social media platforms also monetize the "data goldmine" of their users' behavior and conversations. **Reddit recently disclosed they are making tens of millions per year** to let Google use their users' data to train Google's AI models.

Where are they?

Let's not focus on where they are, let's talk about where YOU are. Location data is very lucrative for data brokers, and most people have no idea how much of it they are providing to companies they have never heard of.

We used two primary sources for this section: The Electronic Frontier Foundation (**EFF, https://eff.org**), a digital civil liberties advocacy; and the US Federal Trade Commission (**FTC, https://ftc.gov/**), the US government's business fairness and consumer protection watchdog.

The FTC recently wrote about a proposed settlement with one data broker, X-Mode (and its successor company Outlogic LLC). **X-Mode is accused of collecting "precise consumer geolocation data"** from many sources, including their own phone apps and those using X-Mode's software development kit (SDK).

X-Mode's SDK gives developers a canned subsystem to handle location data in their apps. It's a way for the developer to add those needed features without spending months to develop their own interface to the phone's location services. What the developers didn't know (or possibly didn't care about) is that the location data is captured in the process by X-Mode's servers for their own use. Consumers of the apps certainly did not know. **According to a 2020 interview with X-Mode's CEO** at the time (which does not appear to be available online anymore), "more than 50 million active people per month are sharing their location every 5 to 7 minutes with X-Mode". The FTC complaint claims "X-Mode daily has ingested over 10 billion location data points from all over the world."

The **FTC points out that collection of the data is only part of the problem**. When X-Code sells such sensitive data, they have a duty to ensure that it is going to be used ethically. In some cases their customer contracts paid lip service to this idea, but there was no verification, follow up, or enforcement by X-Code.

There are many reasons people do not want their location data tracked this way. People visiting certain medical facilities do not want that information to be used against them. As some states are trying to enact laws to make it illegal for women to visit reproductive clinics, even in other states, it is chilling to realize that those states can purchase that data on the open market as soon as they decide they want it.

Regardless of which side of the abortion debate

you are on, consider the ramifications of that level of state interference in citizen lives. What if the next right to be curtailed is something you hold dear? What if it's as simple as reporting every time you visit a dispensary or liquor store or frozen yogurt shop? What if that information is used to increase your insurance premium, or deny an insurance claim altogether?

The Fog

In spite of their name, Fog Data Science provides crystal clarity to their customers about the locations and habits of millions of citizens. **Fog's 2019 marketing materials reveal** that they are collecting billions of data points on over 250 million devices. The data is extremely detailed, near real-time, and historically long-reaching. Their product "Fog Reveal" offers two kinds of search.

- "Area searches" allow **police customers** to specify an area and see what mobile devices that have been detected there in a given time frame.
- "Device searches" let them specify a specific person's device and see the history of their movements. They describe the output as the person's "pattern of life", including their "bed down" location (presumably where they sleep at night).

Fog states that the data is anonymous and no individual's name is attached to the results, only the phone ID. **But police are on record that this is not a hindrance** to fully identifying individuals when Fog Reveal's results are combined with other things the they already know.

The difference between the Fog Reveal product and the warrant the police might get for a suspect's phone location data is just that: the warrant. This incredibly detailed personal information is available indiscriminately without a judge's evaluation. It doesn't even cost very much. The California highway patrol paid just under $10,000 for a year of access, which allowed them up to 600 searches per month.

There are cases where specific legislation has curtailed the use of this data by law enforcement. One example is in **Chino, CA, where police are required to get a judge's order** before using Fog Reveal, unless there are exigent circumstances. But for the vast majority of us, the agencies charged with protecting us are under no such restrictions.

Protect Yourself

Hopefully this dive into the details of how brokers acquire and sell and use your location data has been eye opening. Remember that other very specific data niches are being collected and used against you in similar ways, including financial and health data.

Here are some ways you can minimize the amount of data that is collected on you:

- Use an iPhone instead of Android. Right now, the default user controls on iPhone are more pro-consumer. This might not be true forever, or in all countries, and trusting the **world's most profitable computer company** may seem dubious. **Both platforms have privacy problems**, but iPhone is **currently** better with less user effort.
- Review the privacy settings on your devices. On iPhone go to **Settings > Privacy & Security > Safety Check**. On Android go to **Settings > Security and Privacy > Permissions Manager**. From there you can control which apps have access to which parts of your private data. Of course Uber and Wayze need your location data to function. But some random solitaire game or the Netflix app don't need it.
- Use an ad blocker. On the desktop, **uBlock Origin** is a good choice. For mobile, search the appropriate app store for "ad blockers" and read independent reviews before choosing. In a future issue we'll look more deeply into ad networks and explain why ad blockers essential.
- There are companies such as **Incogni** that will act on your behalf, for a fee, to get your data removed from the databases of hundreds of data brokers.

The most famous line from Jean-Paul Sartre's play "**No Exit**" is, "Hell Is other people." There's a lot for existentialist philosophers to unpack in that statement, but it also directly applies to modern privacy concerns. In the play, three people are forced to live together in Hell, never apart, always subject to observation and judgment from the others.

In our digitally connected lives, corporations and governments are always watching us. Researching just how pervasive these observations are gives one a distinct sense of paranoia. "Should I search that from my regular computer? If my searches become public, how will my friends and family react?" Perhaps we can update Sartre's line to, "Hell is the global digital surveillance panopticon". Stay safe.

Southwest Cyberport

New Mexico's Expert Internet Service Provider since 1994

505-232-7992 | Support: help@swcp.com

5021 Indian School NE, Ste. 600, Albuquerque, NM 87110

Click on bold blue type in browser for links.