Incident Fact Sheet

What does Gravy Analytics do?

Gravy Analytics is a location intelligence and insights company. In November 2023, Gravy Analytics and Unacast merged, creating a location analytics platform. We rely on commercially available, user-consented data for our platform. We license this data from pre-vetted, independent data suppliers. **We do not track smartphones or other device locations.** We do not collect location data directly from individuals, from devices, or from apps.

We validate and analyze the licensed data we receive to create our own proprietary datasets that we sell to our customers. This process includes using our privacy-enhancing technologies, such as PrivacyCheck, which masks sensitive locations. Our customers use this data to gain meaningful insights for their own businesses, such as to inform marketing and digital advertising strategies. Our data is also used for public benefits, such as helping communities with urban planning projects like parks and shopping centers, or assisting researchers in improving emergency evacuation and disaster response planning.

What happened in our recent security incident?

On January 4, 2025, we discovered that a person had accessed Gravy Analytics' AWS cloud storage environment without authorization. This unauthorized person copied some data stored in certain AWS buckets and temporarily made a small subset of that data available on a dark web forum. The dark web is not available through standard search browsers.

We immediately took steps to help ensure the security of our AWS environment and have investigated this security incident with the help of outside cybersecurity experts. We continue to evaluate strategies to further enhance our AWS security.

What data was involved in the security incident?

The security incident involved commercially available data. A limited subset of this data, covering primarily a few days around New Year's 2025, was briefly posted on a dark web forum. The data we license mostly consists of mobile advertising IDs (MAIDs), longitude/latitude, and timestamps. **We do not receive information that can directly identify specific people, and we have no reasonable ability to identify any person.**

A MAID is a software-based identifier associated with a device. Unlike more permanent hardware identifiers like the IMEI number or MAC address, MAIDs are designed to help protect device user identities. The precision of location data we get varies. The data we receive often does not clearly link MAIDs to any location data. This means, for example, that we frequently have location data with a timestamp but no associated device.

Our analysis of the data posted shows that most of the data consists of unlinked data elements that cannot be associated with any device. Even when a MAID is linked to location data, associating a specific person with any of this data would demand significantly more processing and supplementary datasets. The potential for tracking or profiling any person with this data is further limited by the restricted time span it covers. Harm is unlikely as a direct result of this incident.

How do we get device data?

The data we license is user-consented and user-controlled. Our data suppliers get device data when a device user opts in to location sharing or other device activity tracking. Our data suppliers must ensure that appropriate user consent is present. Consistent with our own regulatory obligations, we also perform independent due diligence on our data suppliers to confirm that the data we license comes from devices that have opted in to the collection and transfer of location signals. In other words, device users can freely choose to opt in to or out of data sharing.

What choices do people have about data sharing?

People have several options for controlling the data shared from devices.

Apple device users can –

- Turn location services on or off from the Privacy & Security settings (under Location Services)
- Manage your device activity tracking permissions from the Privacy & Security settings (under Tracking)
    - Note that when you toggle your device tracking permissions on and off, your device MAID is automatically reset.

Android device users can –

- Manage your device's location settings, including turning them on and off and adjusting the accuracy of locations, from the Location settings
- Reset or delete your device's MAID, from the Privacy settings

You can also opt out of certain data uses. You can opt out of our location data sales by using our Opt-Out Form. You will need to provide your device's MAID for us to process the opt-out request, because we are unable to associate MAIDs with people. Your MAID is usually a long

alphanumeric string separated by hyphens, such as AB1234CD-E123-12FG-J123, which may be upper- or lowercase. For Apple devices, you need a third-party app, like My Device ID, to retrieve your MAID. For Android devices, you can find your MAID in the Ads settings.

Many apps on your devices will allow you to opt out of data sales and some other purposes. Information about this process is generally available in the app's privacy policy, typically found in the app settings and linked from the app's listing in the Apple App Store or Google Play.

Questions?

If you have other questions, you may contact consumerdataquestions@unacast.com.

Please direct media inquiries to media@unacast.com.