MOTHERBOARD
TECH BY VICE

Inside the Industry That Unmasks People at Scale

Unique IDs linked to phones are supposed to be anonymous. But there's an entire industry that links them to real people and their address.

By Joseph Cox

July 14, 2021, 5:00am

IMAGE: MICHELLE URRA/MOTHERBOARD

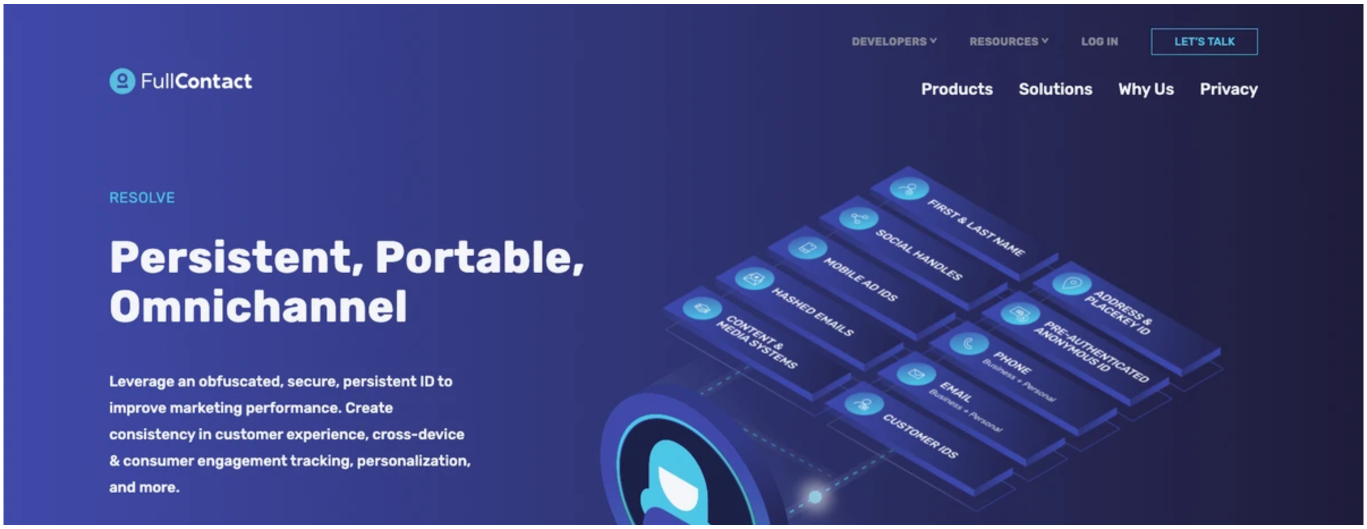
Tech companies have repeatedly reassured the public that trackers used to follow smartphone users through apps are anonymous or at least pseudonymous, not directly identifying the person using the phone. But what they don't mention is that an entire overlooked industry exists to purposefully and explicitly shatter that anonymity.

They do this by linking mobile advertising IDs (MAIDs) collected by apps to a person's full name, physical address, and other personal identifiable information (PII). Motherboard confirmed this by posing as a potential customer to a company that offers linking MAIDs to PII.

"If shady data brokers are selling this information, it makes a mockery of advertisers' claims that the truckloads of data about Americans that they collect and sell is anonymous," Senator Ron Wyden told Motherboard in a statement.

"We have one of the largest repositories of current, fresh MAIDS<>PII in the USA," Brad Mack, CEO of data broker BIGDBM told us when we asked about the capabilities of the product while posing as a customer. "All BIGDBM USA data assets are connected to each other," Mack added, explaining that MAIDs are linked to full name, physical address, and their phone, email address, and IP address if available. The dataset also includes other information, "too numerous to list here," Mack wrote.

A MAID is a unique identifier a phone's operating system gives to its users' individual device. For Apple, that is the IDFA, which Apple has recently moved to largely phase out. For Google, that is the AAID, or Android Advertising ID. Apps often grab a user's MAID and provide that to a host of third parties. In one leaked dataset from a location tracking firm called Predicio previously obtained by Motherboard, the data included users of a Muslim prayer app's precise locations. That data was somewhat pseudonymized, because it didn't contain the specific users' name, but it did contain their MAID. Because of firms like BIGDBM, another company that buys the sort of data Predicio had could take that or similar data and attempt to unmask the people in the dataset simply by paying a fee.


RESOLVE

Persistent, Portable, Omnichannel

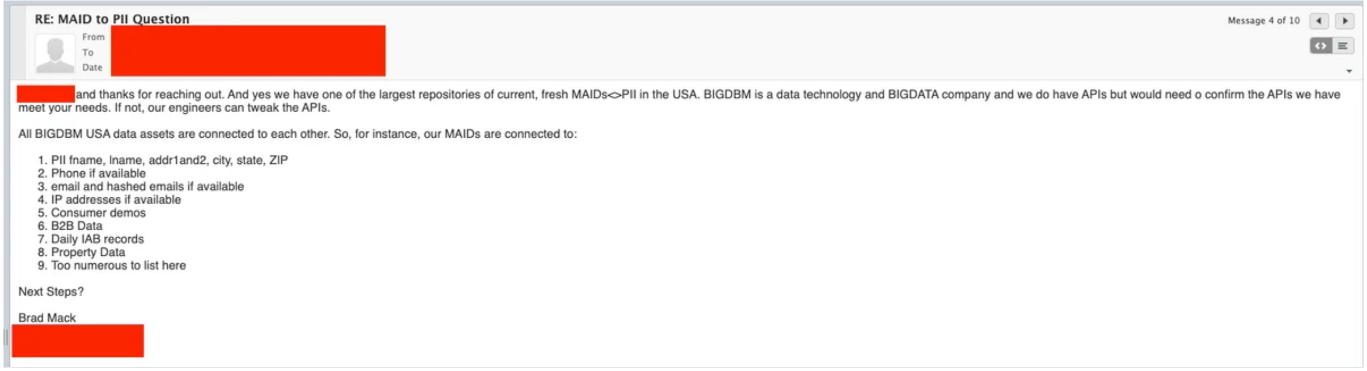
Leverage an obfuscated, secure, persistent ID to improve marketing performance. Create consistency in customer experience, cross-device & consumer engagement tracking, personalization, and more.

currently is at risk of being de-anonymized via unscrupulous companies," Zach Edwards, a researcher who has closely followed the supply chain of various sources of data, told Motherboard in an online chat. "There are significant risks for members of law enforcement, elected officials, members of the military and other high-risk individuals from foreign surveillance when data brokers are able to ingest data from the advertising bidstream," he added, referring to the process where some third parties obtain data on smartphone users via the placement of adverts.

This de-anonymization industry uses various terms to describe their product, including "identity resolution" and "identity graph." Other companies claiming to offer a similar service as BIGDBM include FullContact, which says it has 223 billion data points for the U.S., as well as profiles on over 275 million adults in the U.S.

"Our whole-person Identity Graph provides both personal and professional attributes of an individual, as well as online and offline identifiers," marketing material from FullContact available online reads, adding that can include names, addresses, social IDs, and MAIDs.

"MAIDs were built for the marketing and advertising community, and are tied to an individual mobile device, which makes them precise in identifying specific people," the material adds.



RE: MAID to PII Question

From
To
Date [redacted]

[redacted] and thanks for reaching out. And yes we have one of the largest repositories of current, fresh MAIDs<>PII in the USA. BIGDBM is a data technology and BIGDATA company and we do have APIs but would need o confirm the APIs we have meet your needs. If not, our engineers can tweak the APIs.

All BIGDBM USA data assets are connected to each other. So, for instance, our MAIDs are connected to:

1. PII fname, lname, addr1and2, city, state, ZIP
2. Phone if available
3. email and hashed emails if available
4. IP addresses if available
5. Consumer demos
6. B2B Data
7. Daily IAB records
8. Property Data
9. Too numerous to list here

Next Steps?

Brad Mack
[redacted]

A SCREENSHOT OF THE EMAILED RESPONSE FROM BRAD MACK.

Edwards said that the existence of companies that explicitly link MAIDs to personal information may provide issues under privacy legislation.

"This real-world research proves that the current ad tech bid stream, which reveals mobile IDs within them, is a pseudonymous data flow, and therefore not-compliant with GDPR," Edwards told Motherboard in an online chat.

"It’s an anonymous identifier, but has been used extensively to report on user behaviour and enable marketing techniques like remarketing," a post on the website of the Internet Advertising Bureau, a trade group for the ad tech purchasing Americans' personal data."

Subscribe to our cybersecurity podcast, CYBER.

TAGGED: APPLE, PRIVACY, GOOGLE, CYBER, ANDROID, WORLDNEWS, WORLD PRIVACY

MORE FROM VICE

How Data Brokers Sell Access to the Backbone of the Internet

JOSEPH COX

08.24.21

Tech

A Stalkerware Firm Is Leaking Real-Time Screenshots of People's Phones Online

JOSEPH COX

09.22.21

Tech

Company That Routes Billions of Text Messages Quietly Says It Was Hacked

LORENZO FRANCESCHI-BICCHIERAI

10.04.21

Tech

WhatsApp Co-Founder Is the New Acting CEO of Signal

JOSEPH COX

01.10.22

Tech

A Peek Inside Anom, the Phone Company Secretly Used in an FBI Honeypot

JOSEPH COX

12.02.21

Tech

Trumpworld's Anti–Big Tech App Gettr Still Tracks Users for Facebook

JOSEPH COX

01.11.22

JOBS

PARTNER

VICE VOICES

CONTENT FUNDING ON VICE

SECURITY POLICY

PRIVACY & TERMS

ACCESSIBILITY STATEMENT