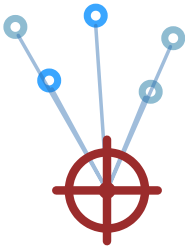


Principal Brief // two-minute read

AD-TECH & REAL-TIME BIDDING

DATA BROKERS

HOUSEHOLD & STAFF



Sold as Ads, Used for Targeting

The advertising data that prices an ad also finds your home, your routine and your family, and it is sold to almost anyone for cents a record.

WHAT HAPPENED

In April 2026 US Central Command told Congress it had received multiple threat reports of adversaries using commercial location data to target or surveil American personnel in theater. Lawmakers made the responses public in May.

WHY IT REACHES YOU

Nothing in that pipeline was built for the military. It is ordinary advertising. The record it builds on a soldier, it builds on you, and it is most complete at home.

THREE THINGS TO TAKE FROM THIS

1

Nothing has to go wrong

No breach, no hack, no mistake. Your phone's location and its advertising ID leave through ordinary apps and ad auctions every day.

2

Nobody checks the buyer

Researchers bought data on service members for as little as twelve cents a record. The market does not ask whether a buyer is an advertiser or an adversary.

3

Your household is the target set

Profiles link spouses, children, addresses, schools and routines. Your own discipline cannot close what your family's phones leave open.

DO THIS

- ☐ **YOU, WITH YOUR SECURITY LEAD**
Treat your broker footprint as a targeting input. Remove the residential, location and people-search records that feed the chain, and repeat it on a schedule, because they come back.
- ☐ **YOU AND YOUR HOUSEHOLD, THIS MONTH**
Turn off the advertising identifier and tighten location permissions on every phone in the house, including those carried by staff.
- ☐ **YOU, WITH YOUR FAMILY OFFICE**
Plan protection around the residence, not only the trip or the public appearance. Home is where your pattern of life is most complete.

NOT THE STORY YOU MAY HAVE HEARD

This is not a military problem that stops at the base gate. The data that exposed personnel in theater is the same kind of data sold about civilians at home.

HOW SURE WE ARE

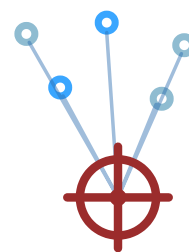
High confidence in how the pipeline works and in the documented cases. Moderate on how fast any one person's records come back after removal, which varies by broker.

THE FULL COMMAND BRIEF FOLLOWS: SOURCES, THE KILL CHAIN, THE STEELMAN, AND ACTIONS FOR YOUR TEAMS.

CB-073

The surveillance-economy kill chain

"The data-broker economy is not a privacy nuisance. It is a targeting system."



Ordinary ad-tech is sold as marketing infrastructure. The same pattern-of-life it produces is a targeting product, priced by the record and sold to whoever pays. On 14 April 2026 a US military command told Congress it had received threat reports of adversaries using it against US personnel. The durable exposure is not the soldier abroad. It is the household at home.

BLUF. The data-broker economy is not a privacy nuisance, it is a targeting system. The ordinary machinery of digital advertising collects precise location and a persistent device identifier, feeds them into an auction seen by many participants, and lets brokers aggregate the result into searchable profiles sold by the record for cents. On 14 April 2026 CENTCOM told Congress it had received multiple threat reports of adversaries exploiting exactly this commercially available location data to target or surveil US personnel in theater: a US command acknowledging, on the public record, that the pipeline has been turned against a protected population.

The governing frame is reach. The target set is not the individual, it is the household. Brokered profiles link spouses, dependents, home addresses, schools, places of worship, and daily routines. The same data that reconstructs a service member's pattern of life reconstructs an executive's, and does so most completely at home, where operational-security discipline is lowest and the assumption of safety is highest.

A system that can find a clearance-holder's child's school is a counterintelligence problem and a physical-security problem at once.

THE SIGNAL // FROM DEMONSTRATED TO OPERATIONAL

CENTCOM TO CONGRESS • 14 APR 2026

CENTCOM reported it received multiple threat reports of adversaries exploiting commercially available location data to target or surveil US personnel in theater. Its written responses were made public with a bipartisan 28 May letter from fourteen members of Congress to the Defense Department's chief information officer, which also recorded that the advertising identifier was still active on government-issued phones. The broker pipeline is now acknowledged as a threat to American forces in an active theater.

DUKE UNIVERSITY • NOV 2023

A Duke study, funded by a US military grant, bought data on active-duty personnel and veterans, including names and home addresses, for as little as twelve cents per record, with little vetting of the buyer. The cost of acquiring a target's identity and address is measured in cents.

OPEN-SOURCE RECORD • 2016 TO 2024

In November 2024 netzpolitik.org, Bayerischer Rundfunk and WIRED used a broker's free sample of 3.6 billion location points to trace devices at no fewer than thirteen sensitive US and NATO military and intelligence sites in Germany. In 2016 a defense contractor traced phones from US military facilities to a staging area for US special-operations forces in northern Syria using commercial location data. The 2018 Strava exposure revealed base layouts and patrol patterns.

MARKET MECHANISM · 2018 TO 2026

The pipeline is the ordinary ad market. Apps and sites collect device location and the advertising identifier and pass them into millisecond real-time-bidding auctions seen by many participants. Brokers aggregate those signals with public records and purchase histories into profiles bought, licensed, or resold, often with little verification of the buyer. The threat is a byproduct of how the consumer internet is monetized.

THE MECHANISM // WHY THE CHAIN DOES NOT BREAK

Four observations form the argument. Each is documented, and the convergence is the thesis.

OBSERVATION 1

Collection is automatic and continuous. The principal does not have to do anything wrong. Location and a persistent identifier leave the device through ordinary apps and the ad auction itself. There is no breach event to detect and no intrusion to block. The exposure is the normal operation of the phone.

OBSERVATION 2

The identifier makes a person followable. Because the advertising ID persists across sessions, a single device can be tracked over time, turning scattered location pings into a route, a residence, and a schedule. Persistence is what converts data points into a pattern of life.

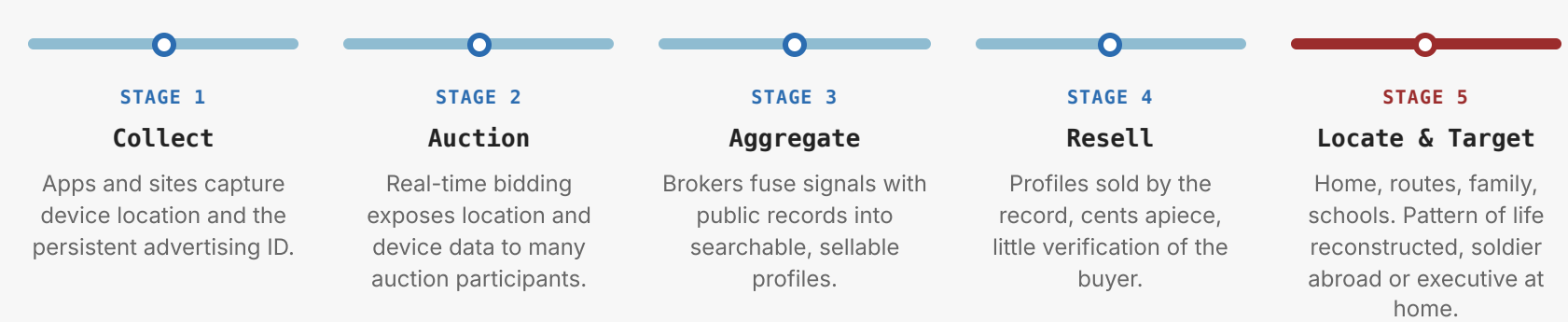
OBSERVATION 3

Scale is cheap and the buyer is unvetted. Sold by the record at cents, with little buyer verification, the market does not distinguish an advertiser from an adversary. The same profile that prices an ad impression locates a person. There is no friction at the point of sale that protects a high-value target.

OBSERVATION 4

The household is the unit, not the individual. Brokered profiles link family members, addresses, and routines, so a principal's own discipline cannot close the exposure. The attack surface is everyone who shares the address and everyone whose device touches the principal's life.

FIGURE 1 // THE SURVEILLANCE-ECONOMY KILL CHAIN



THE CONTESTABLE INPUTS

No stage requires a breach, an intrusion, or a mistake by the target. What a principal controls are the inputs: the device signals that enter at Stage 1 and the brokered records that feed Stages 3 through 5.

FIGURE 2 // THE RECORD IS NOT HYPOTHETICAL

12¢ Per-record price for data on US military personnel. DUKE UNIVERSITY, NOV 2023	13 Sensitive US and NATO sites in Germany traced in one broker's free data sample. NETZPOLITIK.ORG, BR AND WIRED, NOV 2024	14 Members of Congress on the bipartisan letter to the Defense Department CIO. CONGRESSIONAL LETTER, 28 MAY 2026	2018 Year of the directive banning geolocation-sharing apps in operational areas. The advertising ID was still on government phones in 2026. CENTCOM RESPONSES, 14 APR 2026
--	---	---	--

THE STEELMAN // THE CASE THAT THIS IS OVERBLOWN

THE BEST CASE FOR THE OTHER SIDE

- + The data is collected to sell advertising, not to target people, and the overwhelming majority of buyers are ordinary marketers.
- + No single broker set is complete or current. Profiles are noisy, stale, and often wrong at the individual level.
- + Platform changes and advertising-identifier deprecation are already shrinking the available signal over time.

Concede all three: the intent is commercial and any single data set is imperfect. What still fails is that the market sells to the buyer, not to the use, at cents per record with no vetting, so an adversary buys the same product as an advertiser. And the CENTCOM confirmation shows that imperfect data is already good enough to target a protected population. Noise does not protect a household when the price of trying is a few cents.

ASSESSMENT

FIGURE 3 // ANALYTIC CONFIDENCE BY CLAIM

The ad-tech pipeline functions as a targeting system reachable at the household level.	STRONG
The documented record (CENTCOM, the congressional letter, Duke, Germany, Syria, Strava) is verified open-source.	STRONG
Device signals at Stage 1 and brokered records at Stages 3 to 5 are the links a principal can contest.	MODERATE / DOCTRINE
The rate at which any one principal's records repopulate after removal is predictable.	MODERATE / BROKER-DEPENDENT
Regulation will close this market in the near term.	REJECTED / LEVERS POINT AWAY

POSTURE

FOR PRINCIPALS

- ➔ Treat the data-broker footprint as a targeting input, not a privacy preference. The actionable countermeasure is footprint neutralization: removing the brokered residential, location, and people-search records that feed the chain at Stages 3 through 5. With the device settings below, this is what you control.

→ Fix device hygiene as a standing control. The persistent advertising identifier is the key that makes a device followable, so disable it and tighten app location permissions to remove the input at the source. See CB-075 for the device-level checklist.

FOR FAMILY OFFICES

- Defend the household, not the individual. Extend removal and monitoring to spouses and dependents, because the exposure links family members and the shared address. A principal-only program leaves the family member's device and the published school in the data set.
- Assume continuous exposure, not an event. There is no breach to wait for, so treat removal as a recurring cadence rather than a one-time cleanup, since the records repopulate as the market regenerates them.

FOR SECURITY & LEGAL FUNCTIONS

- Read this as a counterintelligence and physical-security problem at the same time, and brief protective and travel planning against the residence, not only the deployment or public appearance.
- Do not wait for regulation to close the market. The federal levers point away from this exact exposure (see CB-074), so the near-term remedy is self-help and procurement discipline, not statute. This is intelligence analysis, not legal advice.

CONFIDENCE HIGH on the mechanism (real-time bidding, the persistent advertising identifier, and per-record resale are documented features of the ad-tech market), on the record (the CENTCOM confirmation, the congressional letter, the Duke study, and the Germany, Syria, and Strava cases are documented in open sources), and on household reach. MODERATE only on the rate at which any single principal's records repopulate after removal, which varies by broker and jurisdiction.

METHOD Revised edition. First published 10 Jun 2026; facts re-verified and analysis revised 20 Oct 2026. Built from open-source anchors, each dated in the text, and cross-read against the regulatory and device-level briefs (CB-074, CB-075) and the residential-targeting line (CB-058, CB-076). Conflict-scenario framing from third-party situational products is excluded by design.

SOURCES CENTCOM written responses to Congress (14 Apr 2026) and the bipartisan congressional letter to the Defense Department CIO (28 May 2026); Duke University Sanford School, "Data Brokers and the Sale of Data on U.S. Military Personnel" (Nov 2023) and the 2021 Sherman report; netzpolitik.org, Bayerischer Rundfunk and WIRED, Databroker Files reporting on Germany (Nov 2024); Wall Street Journal reporting (Apr 2021) on the 2016 Syria tracking case; reporting on the 2018 Strava and Polar exposures; the New York Times "One Nation, Tracked" series; NSA guidance on limiting location data exposure (Aug 2020).

Scope note: this brief rests only on open-source anchors, each dated above; figures should be confirmed against primaries before external reproduction. Advocacy and third-party situational products are excluded, not asserted. This is intelligence analysis, not legal advice.

OBSCUREIQ INTERNAL ANALYSIS // ARCHIVE COMM-073-SURVEILLANCE-ECONOMY-KILL-CHAIN-2026Q2 // XREF [CB-074](#) [CB-075](#) [CB-076](#) [CB-058](#) // ACCESS PUBLIC · PUBLIC-INTEREST RELEASE · REVISED 20 OCT 2026