

Principal Brief // two-minute read

DRONES & AERIAL

RESIDENTIAL EXPOSURE

PATTERN OF LIFE



The Drone Needs Your Address First

An attack drone is useless until someone knows where to send it, and when you will be there. Much of that is sold by data brokers to almost anyone. Delivery is the hard half and is spreading. The finding half is the one you can still shrink.

WHAT HAPPENED

In April 2026 the US military's Middle East command told Congress it had received multiple threat reports of adversaries using commercial location data to target or watch US personnel in an active theater. Drones had already struck the homes of Israel's prime minister in 2024 and the Kurdistan Region's president in March 2026. At home, the FBI broke up two drone-bomb plots, one in 2024 and one in June 2026.

WHY IT REACHES YOU

A drone aimed at a house needs the address; aimed at a person, it needs to know when they are there. Both can be bought in the United States. The same data that sells ads can find a target: only the buyer changes. New federal laws block sales to a few hostile countries; buyers at home face a patchwork. No drone attack on a private American home has been documented. The pieces for one now each have a precedent.

THREE THINGS TO TAKE FROM THIS

1

Finding comes first

Every drone attack needs a location and a time. Brokers sell both, though watching or public records can serve too.

2

The law covers foreigners

New rules stop sales of location data to a few hostile states. Domestic buyers face only a patchwork of rules.

3

You cannot stop the drone

Private owners may not jam or down one. Shrinking what finds you is the lever that is legally yours.

DO THIS

- ☐ **YOU, NOW**
Audit location sharing on every household and staff phone, starting with the advertising ID.
- ☐ **YOU, WITH YOUR FAMILY OFFICE**
Make it harder to link you to your home and your routine, not just to delete records.
- ☐ **YOU, WITH SECURITY**
Know which agency near you holds counter-drone authority, and meet it before you need it.

NOT THE STORY YOU MAY HAVE HEARD

This is not a warning that drone attacks on private homes are imminent. None has been documented in the United States, and the domestic plots aimed at a substation and a public event. It is a claim that each step an attacker would need has now happened somewhere, and that the first step is often the cheapest.

HOW SURE WE ARE

High on each precedent, which rests on official statements, court filings and wide reporting. The military reports concern a war zone, and the domestic plots are a sting and an alleged plot. Inference, not evidence: that the chain will be assembled against a private principal.

CB-076

The coordinates and the delivery: finding is for sale, delivery is spreading



"The surveillance economy supplies the coordinates. The drone supplies the delivery."

This series tracked two threats separately: the commercial location market that tells a stranger where a person lives and moves, and the cheap attack drone that can cover the last stretch to a door. The v1 of this brief, written in June, argued that the two had joined into one chain. Four months on, every link has a precedent. None of those precedents is yet an attack on a private American home, and the brief keeps that distinction in view.

BLUF. The central development since v1 is in the finding half. On 14 April 2026 US Central Command told Congress in writing that it had received multiple threat reports of adversaries exploiting commercial location data "to target or surveil U.S. personnel in theater." That completes a progression: in 2016 a contractor showed military officials it could follow phones from US bases to a Syrian staging site; in 2024 journalists used a free broker sample to follow more than 12,000 devices at 11 military sites in Germany; in 2026 a command in an active theater reported adversaries doing it. Commercial location data is no longer only a theoretical targeting vulnerability, and it became targeting infrastructure without changing its business model: the same data sells ads, and only the buyer changes. The delivery half has precedents too, each from a different context: drones struck the private homes of Israel's prime minister in 2024 and the Kurdistan Region's president in 2026; Ukraine launched 117 drones from trucks near Russian air bases in 2025; and in the United States the FBI stopped a drone-bomb plot against a Nashville substation in 2024 and five people were held over an alleged explosive-drone plot against a White House event in June 2026. No drone attack on a private American home has been documented, and no public record shows brokered data enabling any of these strikes. The transfer to private principals is unproven. The exposure is not, and reducing it is defensible whether or not that threat materializes. Federal law now bars broker sales to a short list of hostile countries; domestic buyers face only a fragmented set of rules.

14 Apr CENTCOM tells Congress of multiple threat reports on adversaries exploiting commercial location data. LETTER, 28 MAY 2026	117 Drones launched from cabins on trucks parked near four Russian air bases, 1 June 2025. SBU, VIA KYIV INDEPENDENT	13 Data brokers warned by the FTC in February 2026 over sales of sensitive data to foreign adversaries. FTC, 9 FEB 2026	0 Documented drone attacks on a private US residence as of October 2026. OBSCUREIQ REVIEW
---	---	--	--

Commercial surveillance becomes targeting infrastructure without changing its business model. Only the buyer changes.

FROM DEMONSTRATION TO EXPLOITATION, 2016 TO 2026

The lawmakers' letter sets out the progression. In 2016 a government contractor briefed senior officials at Joint Special Operations Command on phones it had tracked from US bases to an abandoned cement factory in Syria, reportedly a staging area for US and allied special operations forces. Later, journalists used a free data sample from a US broker to track 12,313 devices that appeared to spend time at or near at least 11 military sites in Germany. Then came the report from an active theater.

THE FINDING HALF, 14 APRIL AND 28 MAY 2026

In unclassified written answers to an inquiry, CENTCOM told Congress it had "received multiple threat reports concerning adversary exploitation of commercial location data to target or surveil U.S. personnel in theater." Fourteen lawmakers led by Senator Ron Wyden and Representative Pat Harrigan made it public on 28 May in a letter to the department's chief information officer. They wrote that such data can be bought from legitimate brokers for a nominal fee and is most useful against people with set routines. CENTCOM said the advertising ID was still not disabled on government phones. What is confirmed is that the command received multiple threat reports. The incidents, methods, adversaries and any resulting attacks are not public, and nothing disclosed shows brokered data enabling a strike. The v1 of this brief called this an official confirmation that brokered data is a live targeting input; the record supports the narrower statement.

HOMES STRUCK ABOARD, 2024 AND 2026

On 19 October 2024 Hezbollah launched three drones at Israel; two were intercepted, and the third hit Prime Minister Benjamin Netanyahu's private house in Caesarea, cracking a bedroom window, without setting off the local sirens. He was not home. On 28 March 2026 a drone damaged the home of Nechirvan Barzani, president of the Kurdistan Region, in Duhok; no one was hurt. Both targets were heads of government with fixed, widely known residences and state air defense nearby.

THE LAUNCH POINT, 1 JUNE 2025

Ukraine's security service moved drones into Russia in wooden cabins on trucks, drove them to points near four air bases, and opened the cabins remotely: 117 drones against aircraft on the ground. It showed at scale what v1 assumed: a launch point can be brought within range of a target and hidden in ordinary traffic until the moment of use.

DOMESTIC PLOTS, 2024 AND 2026

Skyler Philippi was arrested on 2 November 2024 after ordering explosives, from FBI undercover employees, for a drone he planned to fly into a Nashville-area electric substation; he pleaded guilty in September 2025. In June 2026 five people were held over an alleged plan to use explosive-laden drones against the UFC event at the White House on 14 June; a senator was allegedly named as a target in the group's chats. These are a sting and an allegation, and neither aimed at a private home. They show the intent and the method reaching the domestic setting.

THE LAW ON THE COORDINATES, 2024 TO 2026

The Protecting Americans' Data from Foreign Adversaries Act of 2024 bars data brokers from selling sensitive data, geolocation included, to China, Russia, Iran and North Korea or entities they control; the FTC sent warning letters to 13 brokers on 9 February 2026. The Justice Department's data security rule, in force since 8 April 2025, prohibits data brokerage of precise geolocation on more than 1,000 US devices to six countries of concern. Both rules govern sales to foreign adversaries. Neither establishes a general prohibition on domestic purchases; domestic buyers remain subject to a fragmented set of state privacy laws, consumer-protection enforcement and other rules, such as California's data broker deletion platform, which the lawmakers asked the department to use for its personnel.

M1 THREE EXPOSURES, NOT ONE

Finding a principal is three problems, and they are not equally scarce. Where the principal lives is static, and for a fixed residence often already public, so removing it from brokers does not necessarily stop an adversary finding the building. When the principal is there, the pattern of life, and whether they are there now, real-time presence, are dynamic, and for a high-risk principal they can matter more than the address. Commercial location data is what converts a known address into intelligence about presence, absence and routine; that is where the CENTCOM report bites. For many attackers the data is the cheaper part; for a capable adversary, collection, access, planning and operational risk may matter more than either the data or the platform. A broker is also only one source: observation and public information can serve.

FIGURE 1 // THREE LOCATION EXPOSURES, AND WHAT TO REDUCE

EXPOSURE	WHAT AN ATTACKER LEARNS	CHARACTER	DEFENSIVE OBJECTIVE
IDENTITY AND RESIDENCE	Where the principal lives	Static; often already public for a fixed home	Weaken the link between the name and the address
PATTERN OF LIFE	When the principal is usually present or away	Dynamic; built from device histories, vehicles and posts	Reduce the predictability of routine
REAL-TIME PRESENCE	Whether the principal is there now	Dynamic and perishable; the most valuable for timing	Deny timely confirmation of presence

M2 THE RESIDENCE IS THE EASY CASE

A moving person is hard to hit; a house is not. Both residence strikes on record hit buildings whose location was public, not people in transit, and in both cases the principal was elsewhere or unharmed. That is the shape of the residential risk: damage to the place and danger to whoever is in it, from an address that was never secret. It joins this brief to CB-061, where the address is the payload of a swatting call.

M3 THE LAW CLOSES THE FOREIGN CHANNEL, NOT THE DOMESTIC MARKET

The 2024 statute and the 2025 rule are real controls on one route: a hostile state buying Americans' location data in bulk from a US broker. The most likely buyer in a residential case is in the same country, where there is no comprehensive control on acquisition and resale, only state laws, consumer-protection enforcement and opt-out mechanisms that vary by place and by data type. For a principal the practical position is that much of what a broker holds, a stranger can still buy.

M4 THE DELIVERY HALF IS SPREADING, NOT YET HERE

The drone record outside the United States is war and state conflict. Inside it, the cases so far are an FBI sting and an alleged plot, both against infrastructure or a public event. The direction is clear and the domestic count of residential attacks is zero. Posture should be built for the direction without pretending the count is higher.

M5 SAME DATA, DIFFERENT BUYER

The data does not need to change to become targeting data. The same location history supports advertising, audience measurement, investigative research, stalking and hostile intelligence collection; only the buyer's purpose changes. Three things follow. Privacy controls become part of physical protection, not a separate consumer concern. Protecting a principal means examining the links among identity, location, time and associated devices, and deleting an address alone is not enough. And the value of defensive work is measured by how much harder it becomes to connect a principal to a place or a routine, not by how many records disappear.

FIGURE 2 // THE CHAIN: PRECEDENTS, HOW STRONG THE EVIDENCE IS, AND WHAT THE PRINCIPAL CONTROLS

LINK	PRECEDENT ON RECORD	EVIDENCE	WHAT A PRINCIPAL CONTROLS
FIND: WHO AND WHERE	Broker and people-search files; property and court records (CB-061)	Directly demonstrated	Much: address exposure, entity ownership, removal and monitoring
FIX: WHEN, AND NOW	Bases tracked by contractors and journalists; threat reports in theater (CENTCOM, 2026)	Another operational context	Much: advertising IDs, app permissions, posted routines, staff and family discipline
APPROACH: A HIDDEN LAUNCH POINT	Drones hidden on trucks near air bases (Spiderweb, 2025)	Another operational context	Little: awareness of overflights and surveillance before an attack (CB-078)
DELIVER: DRONE AND PAYLOAD	Two leaders' homes struck (2024, 2026); domestic plots (2024, 2026)	Another context; domestic intent only	Little: screening and shelter where a credible threat exists (CB-269)
DEFENSIVE ENVIRONMENT, OUTSIDE THE SEQUENCE	No private right to jam or down a drone; authority sits with government (CB-059)	A constraint on defenders, not an attacker capability	Indirect: a working relationship with the agency that holds the authority
THE ASSEMBLED CHAIN	None against a private US residence	Analytically inferred	Every link above that it can reach

FIGURE 3 // COORDINATES A STRANGER CAN BUY, AND HOW TO SHRINK EACH

SOURCE	WHAT IT GIVES AN ATTACKER	HOW TO SHRINK IT
PEOPLE-SEARCH AND BROKER FILES	Current and past addresses, relatives, phone numbers	Removal and continuous monitoring; removal decays and files repopulate (CB-107)
PROPERTY, COURT AND CORPORATE RECORDS	The address tied to a name, often with a floor plan or photographs	Entity ownership, records suppression where the law allows, care in filings
ADVERTISING AND APP LOCATION DATA	Home, work and routine, as device location histories	Advertising ID off, location permissions and background collection minimal, on every household and staff phone; SDKs, account identifiers and location-sharing services remain
VEHICLE AND PLATE DATA	Movement between places, and where a car sleeps	Awareness of plate readers and connected-car data (CB-040)
POSTS BY FAMILY, STAFF AND VENDORS	Presence, absence and schedule, in real time	Household and staff rules on posting location and routine

► THE TEST

The question is not whether a drone could reach the house; CB-059 settles that it could, and that a private owner may not stop it. The question is how many links of the chain an adversary already holds before buying anything. *If finding the home and fixing the principal's presence costs a stranger a search and a small data purchase, the chain is half built. Those are the links a principal can make expensive, and the dynamic one, presence, usually matters more than the static one.*

FIGURE 4 // THE RECORD BEHIND EACH LINK, 2024 TO 2026

WHEN	EVENT	LINK IT SHOWS	STATUS
19 OCT 2024	Drone hits the Israeli prime minister's private home, Caesarea	Deliver, at a residence	Claimed by Hezbollah; no injuries
2 NOV 2024	Arrest over a planned drone bombing of a Nashville substation	Intent and method, domestic	FBI sting; guilty plea, Sep 2025
1 JUN 2025	117 drones launched from trucks near four Russian air bases	Approach, concealed launch	Claimed by Ukraine's security service
28 MAR 2026	Drone damages the Kurdistan Region president's home, Duhok	Deliver, at a residence	No injuries; no public attribution found
14 APR 2026	CENTCOM reports threat reporting on commercial location data	Find and fix	Disclosed by Congress, 28 May 2026
JUN 2026	Alleged explosive-drone plot against a White House event	Intent and method, domestic	Five held; allegations only

THE STEELMAN // THE CASE THAT THIS IS SPECULATIVE ASSEMBLY

THE STRONGEST VERSION OF THE OPPOSING VIEW

- + The location-data reports concern military personnel in a war zone, not civilians at home.
- + The residence strikes hit heads of government in active conflicts; private principals are not in that category.
- + The domestic cases were an FBI sting and an alleged plot, both aimed at infrastructure or an event.
- + Stacking precedents from different contexts produces a scenario that has never happened.

All true: the assembled chain against a private American principal is an inference. But the recommended defense does not depend on it. Reducing what a stranger can learn about the address and the routine is warranted by stalking, swatting and burglary risk alone (CB-061, CB-107), and it also weakens the first two links here. Waiting for the first domestic case defends against the past; buying hardware a private owner may not lawfully use defends against the wrong thing.

ASSESSMENT

Commercial location data has been used to follow US military personnel from bases.

STRONG / THE 28 MAY LETTER

CENTCOM has received threat reports of adversaries exploiting commercial location data to target or surveil US personnel.

STRONG / CENTCOM, VIA THE LETTER

Explosive-drone attacks have been planned inside the United States.

STRONG / A GUILTY PLEA; A PENDING ALLEGED PLOT

Federal rules bar foreign-adversary sales; no comprehensive domestic control exists.

STRONG / STATUTE AND RULE TEXT

Exposure reduction raises an attacker's effort; it cannot reliably prevent an attack on a known home.

MODERATE / NOT MEASURED

Brokered data enabled a strike on record, or will be used against a private US principal.

NOT ESTABLISHED / INFERENCE

CENTCOM confirmed brokered data as a live targeting input (v1).

NARROWED / THREAT REPORTS, SEE METHOD

POSTURE

FOR PRINCIPALS

- Audit location permissions, advertising IDs and background collection on every household and staff phone. This narrows exposure; it does not end it.
- Treat presence and routine, not only the address, as exposures you control. Against a credible threat, add detection, shelter and escalation plans (CB-269).

FOR FAMILY OFFICES

- Treat address exposure and airspace together: shrink the footprint (CB-061, CB-107); read detection silence as unknown (CB-269).
- Assess identity-to-residence links in brokers and records, schedule disclosures by staff and vendors, and connected-vehicle data. Watch for overflights (CB-078).

FOR SECURITY AND LEGAL FUNCTIONS

- Identify the agency that holds counter-drone authority where the principal lives, which since July 2026 may include trained local police (CB-059), and brief it in advance.
- Plan against the chain, not the drone; skip hardware a private owner may not lawfully operate.

CONFIDENCE High on each precedent, from CENTCOM's written answers, court records and wide reporting. Moderate that exposure reduction raises an attacker's effort; it is not measured, and it cannot reliably prevent an attack on a known residence. Not established: that brokered data enabled any strike on record, or that the chain will be used against a private principal in the United States.

METHOD Revised edition. First published 1 June 2026 as a synthesis of the CENTCOM disclosure with CB-058 and CB-059; brought to the current format with the CENTCOM claim narrowed to threat reporting, and the residence strikes, Spiderweb, the two domestic plots and the 2024 to 2026 rules on foreign sales added. Following external review, the CENTCOM report is placed at the center with the precedents in the lawmakers' letter, each link's evidence is classed, three location exposures are distinguished, and exposure reduction is separated from physical protection. The absence of a domestic residential drone attack reflects an ObscureIQ review of reporting through October 2026.

SOURCES [Nextgov, May 2026](#), on CENTCOM's written answers and the lawmakers' letter; the [letter of 28 May 2026](#), on the 2016 briefing, the German sample and California's platform; [netzpolitik.org, 2024](#), on the German data; [Caesarea, 19 October 2024](#); [AP via Washington Examiner, 28 March 2026](#), on Duhok. [Kyiv Independent](#) on Operation Spiderweb. [US Attorney, Middle District of Tennessee, 4 November 2024](#), and [Justice Department, September 2025](#), on Nashville. [ABC News, 16 June 2026](#), on the White House plot. [Orrick, 12 February 2026](#), on PADFA and the FTC letters; [White & Case](#) on the data security rule. Authority and detection from CB-059 and CB-269. No principal-identifying detail is included.

Scope note: the chain against a private residence is an inference; allegations are reported as allegations. This is intelligence analysis, not legal advice.