AEGEAN INTELLIGENCE GROUP

PUBLISHABLE MARKET RESEARCH · 2026

CLASSIFICATION
PUBLIC

PRODUCT ID
PMR-2026-0714-USA-001

TIMELINESS
DURABLE

DATE
2026-07-14

The Footprint Before the Threat

A Principal's Digital Exposure, Mapped Before an Adversary Maps It

95
AVG EXPOSED PII INSTANCES PER EXECUTIVE

98%
EXECUTIVES WITH PROPERTY INFO VISIBLE ONLINE

$200/DAY
DAILY BROKER FINE FROM AUGUST 1

+41%
VERIFIED PHYSICAL ATTACKS, EARLY 2026

EXECUTIVE DASHBOARD

Most protection programs begin at the threat: the letter, the fixated follower, the anomaly at the gate. The targeting package that precedes the threat is assembled earlier, from sources that are legal to buy and free to browse, and it exists today for essentially every principal whether or not anyone has looked.

THESIS

A principal's physical exposure now begins as a data problem that no intrusion is needed to create. Commercial people-search brokers, breach corpora, property records, and the family's own social output can be assembled into a working targeting package, identity, home address, routine, and an estimate of wealth, by an adversary with no special access. The 2026 evidence base shows this assembly is no longer theoretical: it is documented in the case files of attacks that reached principals at home. Deletion regimes arriving this year, led by California's DROP with mandatory broker compliance from August 1, 2026, raise the cost of the crudest assembly path but leave the surface open. The decision-relevant measure of a principal's exposure is **the live footprint: what can be assembled today, and how quickly it reassembles after removal**, owned and re-measured by one accountable function. A one-time cleanup is not a security state.

KEY STATISTICS

95
Avg exposed PII instances per executive[1]

98%
Executives with property info visible online[1]

100%
Emails recoverable from breach databases[1]

600+
Data brokers registered on DROP[2]

260K+
Deletion requests queued for processing[3]

$200/day
Daily fine per unprocessed request[3]

72 · +41%
Attacks on crypto holders, rising[8,9]

63%
Family offices with no cyber insurance[13]

Scope & method. Open-source intelligence only, verified against allowlisted Tier 1 to 4 sources: regulatory and enforcement disclosure, court and prosecution records, threat-intelligence and industry research, and established press. Criminal matters are drawn from indictments and reporting on charges, are noted as unproven where unadjudicated, and defendants are presumed innocent. Vendor-published exposure statistics are used where methodology is disclosed and are attributed as vendor research. This brief extends AEIG's market-level assessment of the protection industry (PMR-2026-0619-USA-002, The Protection Premium) down to the principal's own decision. Geographic focus is the United States, with European cases where they illustrate a shared pattern. Timeliness: DURABLE.

KEY JUDGMENTS

Six judgments anchor this assessment. Each is tied to the cited evidence in the sections that follow and carries an explicit confidence level.

1 High — A working targeting package on a principal can be assembled from open and commercially available sources alone, no intrusion required. Vendor research across roughly 200 broker and aggregator sites found an average of 95 exposed personal data instances per executive, property information visible for 98 percent, and breach database email coverage of the full sample.[1]

2 Moderate — The open-source footprint is the documented enabling vector in real attacks: the accused in the 2025 Minnesota assassinations worked from a handwritten people-search list, and the attack wave against holders of liquid wealth runs on leaked and brokered identity, address, and balance data. The chain is rarely proven end to end.[5,7,8,11,12]

3 High — The exposure surface is the household, not the individual. Family, household staff, and vendors continuously regenerate location, routine, and wealth signal, and the family offices that concentrate a principal's data are the least defended: 43 percent have experienced a cyberattack, 63 percent carry no cyber insurance, 31 percent have no incident-response plan.[1,13,14,17]

4 High The strongest deletion instrument yet built, California's DROP, becomes enforceable against brokers on August 1, 2026, and still does not close the exposure: only four states maintain broker registries, roughly 750 brokers are registered somewhere with large gaps between state lists, deletion rights stop at state lines, and brokers re-acquire data continuously.[2,3,4]

5 Moderate Suppression works as a maintained cycle and decays as a one-time project. Broker-layer removal shrinks what an adversary can assemble cheaply, but records repopulate within months as brokers re-acquire data; the value sits in the cadence, not any single pass. Moderate because repopulation is documented by practitioners and vendors, not independent controlled study.[1,18]

6 High The decision-relevant metric for a principal is the live footprint: what an adversary can assemble today and how fast it reassembles after removal. That number must be owned by one accountable function spanning physical security, cyber, and privacy; a deletion receipt or an annual audit is a record of the past, not a security state.[1,19]

SECTION 01 · ASSEMBLY

The Package Assembles Itself

Identity, address, family map, property detail, and breach-derived contact data exist for effectively every principal before any adversary acts. The variable is not whether, but how cheaply.

Begin with what exists before any adversary acts. The commercial people-search and data-broker layer holds, for essentially any American principal, a continuously refreshed dossier: current and prior home addresses, phone numbers, relatives and their addresses, property ownership and purchase prices, and often photographs of the home itself. Vendor research published in 2026, examining executives across roughly 200 popular broker and aggregator sites, found an average of 95 instances of exposed personal data per executive; property information was visible online for 98 percent of those examined, exterior images of the property for 92 percent, and email addresses recovered from breach databases covered the entire sample.[1] None of this requires a purchase on a criminal market. It is the retail layer of the surveillance economy, reachable by search engine.

Beneath the retail layer sits the breach corpus. Decades of corporate intrusions have produced a cumulative, searchable body of credentials, contact details, and increasingly, financial signal. The 2025 Coinbase incident is the canonical example for this brief's audience: bribed overseas contractors exfiltrated records on 69,461 customers including names, home addresses, and account balances, the exact fields a physical targeting package needs, and the United States Senate's Joint Economic Committee has put the consumer cost of data-broker breaches alone above 20 billion dollars.[6,7] The newest accelerant is synthesis: 2026 research documents general-purpose AI models returning residential addresses for named executives, sourced from people-search sites and public tax documents, collapsing what was once hours of manual assembly into a prompt.[1]

ASSESSMENT · HIGH CONFIDENCE

For planning purposes a principal should assume the targeting package already exists: identity, address, family map, property detail, and breach-derived contact data are assembled or assemblable from open sources for effectively every principal in the United States. The variable an adversary controls is not whether the data exists but how little effort it costs to compile.

Rationale: *The broker-layer exposure statistics, the breach-corpus coverage, and the documented AI-assembly path are convergent, and each is independently sufficient to supply the core fields of a package.*[1,6,7]

SECTION 02 · PROOF

From Record to Doorstep

The claim that data exposure precedes physical harm no longer rests on inference. It is in the case files.

In the June 2025 murder of a Minnesota state legislator and her husband, the accused is documented to have located victims through people-search and data-broker sites, with a handwritten list of roughly eleven such services and dossiers on dozens of officials recovered from his vehicle.[5] That case involved public officials; the parallel track against holders of liquid wealth is broader and accelerating. Independent trackers logged a record 72 physical attacks on cryptocurrency holders in 2025, up roughly 75 percent year over year, and the tempo rose again in early 2026: 34 verified incidents between January and April against 24 in the same window of 2025, a 41 percent increase, with roughly 100 million dollars in losses across ransoms paid, funds frozen, and failed demands, and a full-year projection near 130 incidents.[8,9] Europe now carries an outsized share of these cases, with France the single most affected country.[8,9]

The method has professionalized around the data. In January 2025 a co-founder of the hardware-wallet maker Ledger and his wife were abducted from their home in France, a finger severed to extract a ransom near 10 million euros.[10] On January 31, 2026, two teenagers drove roughly 600 miles to Scottsdale, Arizona, posed as delivery drivers, and forced their way into a home in an attempted robbery prosecutors value at some 66 million dollars, directed by phone over an encrypted app; a parallel federal indictment describes a Tennessee crew using the same delivery-driver disguise to take 6.5 million dollars in a single incident.[11,12] What connects the cases is the targeting data: profiles built from displays of wealth, public appearances, and leaked or brokered datasets, assembled remotely and executed locally.

ASSESSMENT · MODERATE CONFIDENCE

The open-source footprint is the operative enabling vector in the current attack pattern, and the pattern is growing. Confidence is moderate because the breach-to-doorstep chain is proven in a minority of cases: Minnesota directly, the crypto wave in aggregate. Either way, footprint reduction attacks the cheapest, earliest link in the adversary's chain.

Rationale: *The recovered people-search list in the Minnesota case, the record and still-rising attack counts, the documented identity-address-balance breaches, and the remote-coordination pattern in 2026 prosecutions jointly support the vector claim, with the causal caveat stated.*[5,7,8,9,11,12]

SECTION 03 · HOUSEHOLD

The Family Is the Perimeter

A principal who personally posts nothing still leaks, through family, staff, vendors, and the family office that concentrates it all.

Spouses, children, household staff, contractors, and vendors each carry a fragment of the household's location, routine, and wealth signal, and insurers and security practitioners have documented the pursuit of families as the soft route to a hardened principal.[14] A single geotagged post from a family member, a staff hire announced on a networking profile, or a vendor photographing an event inside the residence publishes what no broker suppression can retract. The 2026 exposure research makes the same point from the data side: the household's property, not the principal's person, is the most consistently exposed object, visible for 98 percent of executives examined.[1]

The structure holding this surface together is, most often, a family office, and the family-office sector remains measurably under-defended relative to what it concentrates. Deloitte's survey found 43 percent of family offices had experienced a cyberattack, rising to 57 percent in North America and 62 percent among offices serving families above one billion dollars in assets; yet 63 percent carried no cyber insurance, 31 percent had no incident-response plan, and only 22 percent ranked cybersecurity among their top risks.[13] Sector reporting now records demand for support spanning medical, physical, and cyber protection together, an acknowledgment that the exposures arrive as one.[17] A family office concentrates the principal's wealth data, travel calendar, property portfolio, and staff records in a lightly governed entity: precisely the single point of assembly an adversary would design.

ASSESSMENT · HIGH CONFIDENCE

Footprint management scoped to the principal alone will fail, because the household regenerates the exposure continuously. An effective program covers the family, resident staff, and recurring vendors, and treats the family office itself as the highest-value single target in the structure.

Rationale: *The documented family-pursuit pattern, the property-level exposure statistics, and the family-office preparedness gaps are consistent, and each points at the household rather than the individual as the operative unit.* [1,13,14,17]

SECTION 04 · SUPPRESSION

What Deletion Buys, and What It Does Not

The strongest deletion machinery ever built becomes enforceable on August 1, 2026. It raises the adversary's cost. It is not a perimeter.

California's Delete Request and Opt-out Platform, DROP, run by the state privacy agency, went live to consumers on January 1, 2026: a single request directing every broker registered in California, more than 600, to delete the requester's personal information.[2] The enforcement half arrives now: from August 1, 2026, brokers must pull and process the queued requests, more than 260,000 of them, on a 45-day cycle, facing fines of 200 dollars per request per day for failure.[3,18] For a principal with California nexus, this is the cheapest large-scale suppression instrument ever available, and its first compliance data will land within this brief's horizon.

The limits are structural. Only four states, California, Vermont, Texas, and Oregon, maintain broker registries at all; analysis of the registries found roughly 750 brokers registered somewhere, with large numbers absent from any given state's list, so the deletion right thins out at state lines and misses unregistered brokers entirely.[4] Profession-specific statutes such as New Jersey's Daniel's Law protect judges and police, and its core liability question was still before the state supreme court as of March 2026.[15] The Federal Trade Commission has barred individual brokers from selling sensitive location data, category by category.[16] And beneath all of it runs the mechanism that defeats one-time cleanups: brokers re-acquire data continuously from public records, purchases, and fresh breaches, so removed records repopulate within months.[1,18] Deletion is real leverage. It is not a perimeter, and it was not designed for the executive and private-principal class, who inherit it incidentally.

ASSESSMENT · HIGH CONFIDENCE

The 2026 regulatory wave raises the adversary's assembly cost meaningfully for covered persons and jurisdictions, and a protection program should exploit it fully. It does not substitute for maintained suppression: coverage is partial by state, broker, and data category, and repopulation is continuous. Treat DROP and its analogues as one recurring input to a footprint program, not the program.

Rationale: *The platform's scale and penalty structure are documented, and so are the four-state registry limit, the registration gaps, the unresolved litigation, and the re-acquisition dynamic that together bound what deletion alone can deliver.*[2,3,4,15,18]

SECTION 05 · DECISION

The Baseline Decision

Does anyone currently know what an adversary could assemble on the household today, and is anyone accountable for shrinking it and keeping it shrunk?

The instrument is a footprint baseline: a point-in-time, adversary-perspective assembly of what open and commercial sources yield on the principal, family, staff, and properties, graded by what it enables, address confirmation, routine prediction, wealth estimation, approach design. The baseline converts an ambient anxiety into a measured surface, and it names the metric that matters thereafter: how much of the package remains assemblable, and how quickly removed elements reassemble.

Sequencing follows from the evidence. The baseline comes first, because suppression without measurement cannot be verified. Suppression runs as a cycle, broker removals including the DROP channel where nexus exists, takedown requests, breach-exposure rotation, household social-media and vendor policy, on a stated cadence rather than as a project with an end date.[2,18] Monitoring closes the loop: re-audit against the baseline, alerting on new exposure, and integration with whatever physical program exists, so the detail at the gate and the data upstream of it are read by the same owner. AEIG's market-level assessment reached the same terminus from the spending side: protection budgets fail at the seams between physical, cyber, and privacy, and the differentiator is a single accountable owner of the combined exposure.[19] The footprint baseline is the first artifact that owner should hold.

ASSESSMENT · HIGH CONFIDENCE

Commission the baseline, assign the owner, and manage the live footprint as a standing metric with a stated review cadence. A household that has never measured its footprint is not unprotected; it is unmeasured, operationally the same fact. The spend is modest against any physical detail, and it addresses the link every documented case here exploited first.

Rationale: *The assembly evidence, the case pattern, the household-surface finding, and the bounded value of deletion converge on measurement plus maintained suppression under single ownership as the highest-leverage first action.*[1,5,8,19]

SECTION 06 · OUTLOOK

Three Scenarios, Twelve Months

Construction confidence reflects analytical quality, not probability. Each scenario carries a triggering signal for the question this brief raises: does the open-source footprint stay cheap to assemble.

Baseline · Exposure Persists, Deletion Bites Partially

CONSTRUCTION CONFIDENCE: HIGH · VELOCITY: GRADUAL

DROP compliance from August 1 produces measurable deletion at registered California brokers and the first enforcement actions against laggards; a small number of states move copycat legislation. The attack tempo against holders of liquid wealth holds at or above the 2025 record, consistent with the early-2026 rise. The broker layer thins where regulated and regrows where not; the assembly cost for a competent adversary rises modestly and unevenly. Most family offices remain unmeasured and unowned on this surface.

SIGNAL TO WATCH: CPPA COMPLIANCE AND ENFORCEMENT DATA AFTER AUGUST 1; WHETHER VERIFIED WRENCH-ATTACK COUNTS THROUGH Q4 2026 TRACK THE ROUGHLY 130-INCIDENT PROJECTION.

Deterioration · The Assembly Industrializes

CONSTRUCTION CONFIDENCE: MODERATE · VELOCITY: RAPID

A high-profile attack on an executive or private principal is publicly and specifically attributed to a named broker dataset or breach, crystallizing liability and duty-of-care exposure, or AI-assembled targeting dossiers surface as a documented criminal service, collapsing the adversary's cost floor faster than deletion regimes raise it. Insurers reprice personal-security and kidnap-and-ransom cover; demand for suppression and protective-intelligence services spikes into a thin supplier base.

SIGNAL TO WATCH: A PROSECUTION OR INVESTIGATION PUBLICLY NAMING A DATA SOURCE AS THE TARGETING BASIS FOR AN ATTACK ON A PRINCIPAL; MARKETED CRIMINAL TOOLING FOR AUTOMATED PERSON-TARGETING DOSSIERS.

Stabilization · Suppression Becomes Standard Practice

CONSTRUCTION CONFIDENCE: LOW-MODERATE · VELOCITY: STRUCTURAL

DROP's first compliance cycle demonstrates real deletion at scale; additional states adopt registry-plus-deletion regimes and a federal standard gains motion; footprint baselines and maintained suppression become a normal line item in executive-protection and family-office budgets the way penetration testing became normal in corporate security. The assembly cost for the crudest packages rises durably, pushing adversaries toward harder paths.

SIGNAL TO WATCH: MULTI-STATE OR FEDERAL DELETION LEGISLATION ADVANCING; PROTECTION AND FAMILY-OFFICE INDUSTRY SURVEYS SHOWING FOOTPRINT SUPPRESSION AS A STANDARD ENGAGEMENT LINE.

ASSESSMENT · MODERATE CONFIDENCE

The most probable twelve-month path is Baseline: partial, jurisdiction-bound deletion gains against a professionalizing threat, leaving the footprint decisive. Deterioration is the fast risk, a single publicized data-to-doorstep attribution away. The household that baselines and maintains its footprint is better positioned in every scenario, making the Section 05 decision robust to the outcome.

Rationale: *The enforcement calendar is fixed and near, the attack-tempo data is current and directional, and the regulatory diffusion rate is the slowest-moving variable in view.*[2,3,8]

SOURCE REGISTRY

1. Nisos, "Executive Digital Exposure: 2026 Report Findings," 2026.
2. California Privacy Protection Agency, "Delete Request and Opt-out Platform (DROP)," 2026.

3. Tech Times, "California DROP Enforcement Hits Aug. 1: Data Brokers Face $200-Per-Day Fines," 2026-07-08.
4. Electronic Frontier Foundation (with Privacy Rights Clearinghouse), "Why Are Hundreds of Data Brokers Not Registering With States?," 2025.
5. Electronic Privacy Information Center (EPIC), "Data Broker Harms to Public Officials," 2026.
6. U.S. Senate Joint Economic Committee, "Data Broker Breaches Cost U.S. Consumers More Than $20 Billion," 2026.
7. Bloomberg, "Coinbase Says Former Agent Arrested in India After Exchange Hack," 2025.
8. CertiK, "2026 Wrench Attacks Overview," 2026.
9. CoinDesk, "Crypto Crime Is Getting Violent: Wrench Attacks Jumped 75%," 2026-02-02.
10. France 24, "Suspect in French Crypto-Sector Kidnappings Arrested in Morocco, Justice Minister Says," 2025.
11. U.S. Department of Justice, U.S. Attorney's Office, Northern District of California, "Three Tennessee Men Indicted on Robbery, Kidnapping, and Conspiracy Charges Related to a $6 Million Cryptocurrency Robbery Spree," 2026.
12. The Block, "Teens Face Felony Charges After 600-Mile Drive to Allegedly Attempt a $66 Million Crypto Robbery," 2026.
13. Deloitte Private, "The Family Office Cybersecurity Report 2024," 2024.
14. Aon, "Pursuing Families to Target High-Net-Worth Individuals," 2022.
15. New Jersey Monitor, "NJ Supreme Court Hears Arguments Over Daniel's Law," 2026.
16. Federal Trade Commission, "FTC Takes Action Against Gravy Analytics and Venntel for Unlawfully Selling Location Data," 2024.
17. RBC Wealth Management & Campden Wealth, "The North America Family Office Report 2025," 2025.
18. National Law Review (Robinson & Cole LLP), "The Compliance Wave Is Coming: Data Brokers Brace for DROP Deletion Requests," 2026.
19. Aegean Intelligence Group, "The Protection Premium (PMR-2026-0619-USA-002)," 2026-06-19.

AEGEAN INTELLIGENCE GROUP

Publishable Market Research

Timeliness: DURABLE.

Classification: PUBLIC.

contact@aegeanintel.com · aegeanintel.com