

Principal Brief // two-minute read

- RESIDENTIAL EXPOSURE
- EXECUTIVE PROTECTION
- DATA REMOVAL



Locking the Digital Front Door

A stranger with intent needs one thing before anything else can happen: your address. That is the cheapest part of the chain to take away, and the only part you can take away before the stranger exists.

WHAT HAPPENED

In June 2025 a man shot four people in their homes across two Minneapolis suburbs, killing a state representative and her husband, and went to two more legislators' houses the same night. He lived about fifty miles away. Investigators found notebooks naming more than forty-five officials, one address written beside a name, and a list of eleven people-search websites annotated with which were free and what each one required. He wrote the lookup down as a procedure.

WHY IT REACHES YOU

Because the same records list you, your relatives, your other properties, and often your routine, and the population using them is growing while becoming harder to watch: of the violent rhetoric aimed at public officials, only 1.4 percent came from anyone tied to an extremist organization. There is no group to monitor. There is only the record they all start from.

THREE THINGS TO TAKE FROM THIS

- 1

It is not about distance

Most attackers live close. What they lack is a relationship, and that is what makes them need a lookup.
- 2

Locals use the sites too

Believing you know where someone lives is not a confirmed address. Brokers supply the confirmation, and the second home, and the relatives.
- 3

Not a silver bullet, still a lock

You lock the front door even though a neighbor could break a window. Removal closes the easiest path, not every path.

DO THIS

- ☐

YOU, THIS QUARTER

Have someone look you up the way an adversary would, and price what it cost them. That number is your exposure.
- ☐

YOU, WITH YOUR FAMILY OFFICE

Extend removal to relatives, staff, and second properties, and treat it as maintenance. Records repopulate.
- ☐

YOU, WITH YOUR SECURITY LEAD

Fund both layers. Removal reaches the stranger who has not appeared yet; the perimeter reaches the one already there.

NOT THE STORY YOU MAY HAVE HEARD

This brief does not claim attackers are mostly strangers from far away. Most lone-actor attacks happen within ten miles of the attacker's home. It claims something narrower: whatever the distance, someone with no relationship to you has to look you up first, and that step is the one you can make expensive.

HOW SURE WE ARE

High on the case record, the attacker studies, and the legal precedent. Moderate that removal lowers the odds for any one person: the mechanism is documented, the effect size has never been measured, and anyone quoting one is guessing.

CB-058

The Internet Replaced Proximity



"The question is not how far the attacker lived. It is how he learned which house was yours."

On the night of 14 June 2025 a man drove between Minneapolis suburbs and shot four people in their homes. He lived about fifty miles away. In his vehicle investigators found notebooks naming more than forty-five officials, a wider list of roughly seventy people, one victim's home address written beside her name, and a list of eleven consumer people-search websites annotated with which ones were free and what each one required. He was not a stranger to the state. He was a stranger to the people, and he closed that gap with a lookup he had priced in advance.

BLUF. The residential-exposure argument is usually made about distance: the attacker comes from far away, so local familiarity is no defense. The evidence supports something narrower and more useful. Distance varies, and in the aggregate most lone-actor attacks are close to home: Gill and Corner's residence-to-crime study of 122 attacks by 70 individuals across the United States and western Europe found 56.5 percent occurred within ten miles of the attacker's home and 36 percent within two. What does not vary is the need to know where to go. The United States tail is long, with a mean journey of 155 miles against 15.5 in Europe and about a quarter of American cases beyond 100 miles, and the Secret Service's study of 173 mass attacks between 2016 and 2020 found that in 53 percent the attacker had no known affiliation with the location. Boelter, at fifty miles, still wrote down eleven lookup services. The nearby stranger and the cross-country stranger use the same tool.

The governing frame: digital removal is not a silver bullet and should not be sold as one. It is the lock on the digital front door, and a locked door is worth having even though a neighbor could still break a window. Removing a principal's home address, family links, property records, and routine from the people-search layer closes the easiest and most scalable path to the door, which is the path a stranger with intent and no relationship must use, whether that stranger is fifty miles away or two thousand. The choice is not between data removal and physical security. A program needs both, and only one of them can be done before the actor exists.

Motive explains why someone acts. It never explains how they knew which house to drive to.

MINNESOTA LEGISLATORS • 14 JUN 2025

Senator John Hoffman and his wife Yvette were shot at their home shortly before 2 a.m. and survived; Representative Melissa Hortman, the House Democratic caucus leader, and her husband Mark were killed at about 3:30 a.m. The suspect went to the homes of two more legislators the same night. Federal filings record notebooks with the names of more than forty-five state and federal officials, a broader list of roughly seventy people including abortion providers and advocates, Hortman's home address written next to her name, and a list of eleven data-broker and people-search sites with notes on which were free and what data each demanded. He wore a silicone mask and a police uniform, and the manhunt ran about thirty-six hours. This is the clearest documented instance of the locate stage being written down as a procedure.

JUDGE ESTHER SALAS • 19 JUL 2020

A gunman came to the New Jersey home of a federal judge, killed her twenty-year-old son Daniel Anderl and wounded her husband Mark. A list of judges was found in the attacker's rental car. The case produced the Daniel Anderl Judicial Security and Privacy Act, enacted in December 2022, which bars federal agencies and private companies from publishing federal judges' personal information, requires its removal on written request, and prohibits data brokers from trading it. That is the point worth carrying: for one protected class, removal is not a service anyone had to be persuaded to buy. It is federal law, passed because a child died.

THE LONG TAIL • 2011 TO 2022

The remote cases are real and they cluster at the violent end. A man traveled from Idaho to Washington and fired on the White House in 2011. A man traveled from Illinois to Virginia and shot Representative Steve Scalise and others in 2017. Sixteen pipe bombs were mailed to Democratic figures nationwide from Florida in 2018, after the sender had spent months raging online. A man flew from California to Maryland and was arrested near Justice Kavanaugh's home in 2022. None of these actors had local standing, local grievance history, or prior contact to notice, which is exactly the profile relationship-based and perimeter security handles worst.

THE BASE RATES • 1990 TO 2020

Three figures frame the population. Gill and Corner, studying 122 attacks by 70 lone actors since 1990, found a mean residence-to-crime distance of 155 miles in the United States against 15.5 miles in Europe, with about a quarter of American attacks beyond 100 miles and a classic distance-decay curve underneath. The Secret Service found no known affiliation with the attacked location in 53 percent of 173 mass attacks from 2016 to 2020. ObscureIQ's reading of a Reuters analysis of traceable death threats to election officials puts 43 percent as originating outside the target's state. Together they describe a population that is mostly local and reliably relationship-free.

THE WIDENING POOL • OCT 2021 TO SEP 2025

The Institute for Strategic Dialogue, publishing on 3 February 2026 from about 800,000 posts across X, Reddit, Bluesky, YouTube and thousands of forums, found violent rhetoric against leading United States public officials up more than threefold, and up 241 percent comparing October 2021 to September 2022 against October 2024 to September 2025, with Republican-affiliated targets up 364 percent and Democratic-affiliated up 124 percent. The number that matters operationally is the affiliation figure: 79 percent of the threatening content came from people with no known extremist-group ideology and only 1.4 percent involved anyone tied to an extremist organization. Watching organizations no longer finds the actor.

SO WHAT The actor pool is growing, almost none of it is affiliated with anything to watch, and every member of it needs the same thing before acting: an address.

THE MECHANISM // WHERE THE CHAIN IS CHEAP TO BREAK

THE LOCATE STAGE

The chain runs radicalize, locate, travel, act. Radicalization is remote and hard to see. Travel leaves no local footprint to flag. Arrival at the door is where the perimeter finally engages, at the highest cost and the lowest margin for error. Between intent and arrival sits the one stage that is cheap to attack and does not require knowing who the actor is: the point at which a name becomes a street address. Degrade the residential map and an actor with full intent still has an unsolved locate problem.

The objection that everyone in the district knows where the official lives is answered by the case itself. Boelter lived about fifty miles from his victims and still enumerated eleven lookup services with notes on cost. Local belief is not the same as a confirmed address, and an attacker acting on belief risks the wrong house. Brokers supply confirmation, the current address rather than the remembered one, second properties, relatives, and phone numbers. Removal takes away the confirmation step, which is what converts a rumor about where someone lives into an operational plan.

WHY REMOTE ACTORS ESCALATE MORE

Three things compound for the actor with no local presence. Travel is itself a commitment signal, so the ones who do it have already cleared a higher bar of intent. Distance supplies anonymity, with fewer social ties and less local scrutiny near the target. And open data removes the geographic limitation that used to make remoteness protective for the target. The result is a smaller population that is disproportionately dangerous and disproportionately dependent on the data layer, because it has nothing else to work from.

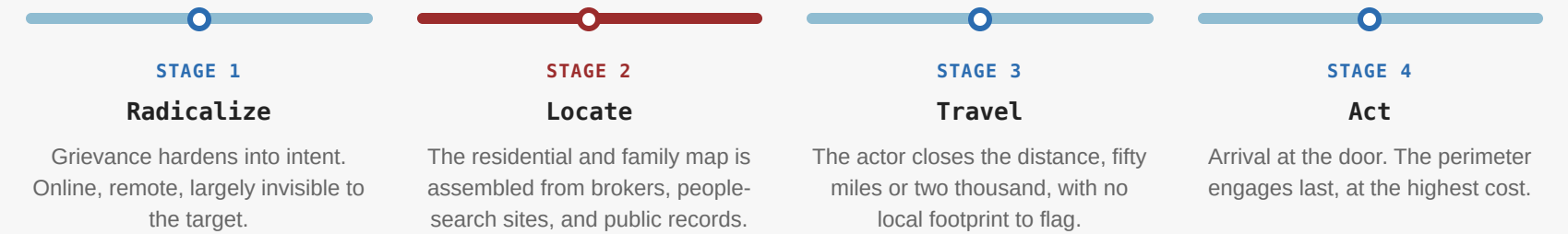
THE ESCALATION LADDER

Most of these cases do not begin with violence. They begin with doxing, when a home address, relatives, and contact details are posted; move to harassment by mail, phone, or platform; move again to stalking and surveillance, when someone visits the home or learns the daily schedule; and only then reach physical action. Each rung depends on the same underlying record. Removing the record early does not just prevent the last rung, it shortens the funnel, because the harassment and surveillance stages are where a diffuse grievance becomes a specific target.

WHAT REMOVAL DOES NOT DO

It does not address the insider, the estranged relative, the former employee, or the neighbor who has genuine proximity knowledge. Those are a different category of risk requiring physical security and behavioral detection, and a brief that pretends otherwise is selling something. Removal also decays: records repopulate, new sources appear, and a one-time project produces a temporary result. Treat it as recurring maintenance with monitoring attached, not a purchase.

FIGURE 1 // THE CHAIN, AND WHERE INTERDICTION IS CHEAP RATHER THAN LATE



THE WINDOW

Stage 2 is the only stage that can be attacked before the actor exists, without knowing who they are, and at a cost measured in subscriptions rather than personnel.

FIGURE 2 // WHAT THE DATA LAYER ENABLES, AND WHAT REMOVING IT FORECLOSES

THREAT	HOW THE DATA LAYER ENABLES IT	WHAT REMOVAL FORECLOSES
DOXING AND SWATTING	Address found on people-search sites or in leaked data, then republished to an audience	Removes the principal from the map an online mob or a hoax caller works from
SCHEDULE-BASED APPROACH	Public event listings, donor records, and scraped calendars establish where the principal will be and when	Limits the ability to time or stage an approach rather than improvise one
FAMILY AND SECONDARY TARGETING	Brokers list relatives, household members, and additional properties beside the principal	Shields the reachable node when the principal is hardened, including second homes and rentals
SURVEILLANCE AND DRY RUNS	A street address supports a recon route, repeat drive-bys, and pattern building before any contact	Cuts off planning and rehearsal, the stages where intent becomes capability
WRONG-TARGET HARM	Stale or incorrect broker records point an actor at a previous address or a similarly named person	Reduces mistaken-identity harm to whoever now lives there or shares the name

FIGURE 3 // FOUR NUMBERS

11 People-search and data-broker sites listed in the Minnesota suspect's notebook, annotated by cost. FEDERAL FILINGS, JUN 2025	53% Of 173 mass attacks, the attacker had no known affiliation with the location. US SECRET SERVICE NTAC, 2016 TO 2020	155mi Mean US lone-actor journey to attack; about a quarter exceed 100 miles, against 15.5 miles in Europe. GILL & CORNER, RESIDENCE-TO-CRIME STUDY	1.4% Of threatening content came from anyone tied to an extremist organization. There is no group to watch. ISD, 3 FEB 2026
--	---	--	--

► THE PRACTICAL TEST

The question is not whether a determined actor could find the address some other way. It is *whether the cheapest path is still open*, and whether anyone has checked this quarter.

THE BEST CASE FOR THE OTHER SIDE

- + Most lone-actor attacks are local. The distance-decay curve is steep, with over half occurring within ten miles of the attacker's home, so a doctrine built on the traveling stranger is aimed at the tail rather than the body of the distribution.
- + A determined actor has other channels: property records, voter files, court filings, social media, a friend of a friend. Closing the broker layer closes one of several.
- + Rising online rhetoric is not rising physical risk. Most threats never become action, and a threefold increase in violent posts is not a threefold increase in attacks.

All three land, and the third is the reason this brief does not present the rhetoric figures as a body count. The answer to the first is that the local actor also used the brokers: at fifty miles, with victims he could plausibly have located other ways, the Minnesota suspect still wrote down eleven services and noted which were free. Removal is not aimed only at the tail, it raises the cost of the locate stage across the whole distribution, and it is the only stage that can be attacked before an actor is identifiable. The answer to the second is that closing one channel is what security is: nobody declines to lock a door because a window exists. What removal claims is narrower than the marketing around it and stronger than the objection allows. It closes the easiest, cheapest, most scalable path, it is the only control that works on an actor nobody has met, and for federal judges the United States Congress already decided it was worth legislating.

ASSESSMENT

FIGURE 4 // ANALYTIC CONFIDENCE BY CLAIM

An attacker's target map was assembled from named people-search services, written down and annotated in advance.	STRONG / FEDERAL FILINGS, JUN 2025
Attackers frequently have no relationship to the target or the location they attack.	STRONG / NTAC, 53 PERCENT OF 173 ATTACKS
The locate stage is the earliest and cheapest interdiction point, and the only one that does not require identifying the actor.	STRONG / STRUCTURAL
The threatening population is overwhelmingly unaffiliated, so organizational monitoring does not find it.	STRONG / ISD, 1.4 PERCENT AFFILIATED
Removal is already established as a remedy in law for one protected class.	STRONG / DANIEL ANDERL ACT, DEC 2022
Removal reduces the probability of an attack on any individual principal.	MODERATE / MECHANISM IS DOCUMENTED, EFFECT SIZE IS NOT MEASURED
How much the widening rhetoric pool raises one principal's physical risk.	MODERATE / RHETORIC IS A POOL INDICATOR, NOT AN ATTACK COUNT
Attackers are predominantly non-local, so distance is the operative variable.	REJECTED / MOST ATTACKS ARE CLOSE TO HOME; RELATIONSHIP, NOT DISTANCE, IS THE VARIABLE
Removal substitutes for physical security or behavioral detection.	REJECTED / DIFFERENT CATEGORY OF RISK, AND THE INSIDER IS UNTOUCHED BY IT

FOR PRINCIPALS

- Treat home address, family links, property records, and routine as the first line item, ahead of visible perimeter spend. The door is the last defense and the cheapest one to have already handled.
- Do not accept the framing that this is removal versus physical security. Fund both, and understand which threat each one answers: removal reaches the stranger who has not appeared yet, physical measures reach the person already at the gate.
- If you are publicly identifiable with a contested position, assume the locate stage currently costs an adversary a few dollars and an afternoon, and act on that assumption now rather than after an incident.

FOR FAMILY OFFICES

- Extend removal to family members, household staff, and secondary properties. Brokers list relatives beside the principal, and the family member is routinely the reachable node once the principal is hardened.
- Treat removal as recurring maintenance with monitoring, not a project with an end date. Records repopulate, new aggregators appear, and a clean result from last year is not a clean result now.
- Audit what the principal's own public footprint discloses about schedule: event listings, donor records, published calendars, and the routines visible in social posts. Address suppression does little if the calendar is open.

FOR SECURITY & LEGAL FUNCTIONS

- Model the unaffiliated stranger with no prior contact and no local grievance history, because that is the profile with no warning signs to detect, and pair it with, rather than substitute it for, the insider and proximity model.
- Track the escalation ladder deliberately: doxing, harassment, surveillance, action. Log and preserve the early rungs, because the material that later demonstrates a pattern is routinely deleted, and the record you keep in week one is the evidence in month nine.
- Where a written target artifact appears in a case, treat it as the clearest available evidence of the locate stage and use it to justify data-layer spend to leadership. Note also what the Daniel Anderl Act does and does not cover, since the statutory protection reaches federal judges and not corporate principals or state legislators. This is intelligence analysis, not legal advice.

CONFIDENCE High that a written, annotated people-search target list was recovered in the June 2025 Minnesota case, which rests on federal filings as reported by The Record and the Minnesota Star Tribune. High on the Secret Service figure, which is the report's own wording about affiliation with the location rather than a measure of distance. High on the Gill and Corner distance findings, which include the point that cuts against a distance-first framing: most lone-actor attacks occur close to home even though the American mean is pulled to 155 miles by a long tail. High on the ISD figures and on the terms of the Daniel Anderl Act. Moderate that removal reduces the probability of an attack on any given principal: the mechanism is documented case by case, but no study measures the effect size, and this brief does not claim one. The Reuters figure of 43 percent of traceable threats originating out of state is carried from ObscureIQ's own citation of the Reuters "Anatomy of a Death Threat" reporting and was not independently reconfirmed for this edition; it is the one number here a reader should treat as second-hand. The specific people-search brands in the notebook are not enumerated because published reporting establishes the count and the annotation but not a verified list of names.

METHOD Revised edition. First published 3 May 2026; facts re-verified and analysis revised 10 September 2026. This edition moves the argument from distance to relationship, which is where the evidence actually sits, and anchors it in the June 2025 Minnesota case in which the locate stage was written down. It adds the residence-to-crime literature including the findings that work against a distance-first reading, adds the Daniel Anderl Act as the precedent that removal is already a legislated remedy, adds the enabling table and the escalation ladder, states plainly what removal does not reach, and separates the rhetoric figures from any claim about attack frequency. Built from federal filings as reported, the Secret Service and academic studies, ISD research, and ObscureIQ's own legislator-facing analysis. Cross-read against CB-059, CB-076, CB-082, and CB-152.

SOURCES [The Record on the data-broker list in the federal filings](#) (June 2025) and the [Minnesota Star Tribune on the people-search services recovered](#) (19 June 2025). US Secret Service National Threat Assessment Center, [Mass Attacks in Public Spaces: 2016 to 2020](#) (January 2023). Paul Gill and Emily Corner et al., ["Lone-Actor Terrorists: A Residence-to-Crime Approach"](#), Studies in Conflict & Terrorism. Institute for Strategic Dialogue, ["Tick tock traitor: the rise of violent rhetoric targeting US public officials"](#) (3 February 2026). Daniel Anderl Judicial Security and Privacy Act (enacted December 2022); background via [Rutgers Law](#). Reuters, "Anatomy of a Death Threat", as cited in ObscureIQ's legislator analysis.

Scope note: this brief argues that the locate stage is the cheapest interdiction point, not that removal prevents attacks. No study measures how much removal changes outcomes for an individual, and any vendor claiming otherwise is overstating the record. Removal does not address insiders, estranged relatives, or actors with genuine proximity knowledge, and it decays without maintenance. Rhetoric-volume figures indicate a widening actor pool, not a count of attacks. Case details rest on federal filings as reported, which reflect the government's account in matters that were pending. This is intelligence analysis, not legal advice.

OBSCUREIQ INTERNAL ANALYSIS // ARCHIVE COMM-058-NON-LOCAL-THREATS-2026Q2 // XREF [CB-059](#) [CB-076](#) [CB-082](#) [CB-152](#) // ACCESS
PUBLIC · PUBLIC-INTEREST RELEASE · REVISED 10 SEP 2026

CB :: RESIDENTIAL EXPOSURE & PHYSICAL THREATS

PRINCIPAL PROTECTION & PRIVACY INTELLIGENCE

PRINCIPAL DISTRIBUTION