

# ASTER PRIVACY

---

Map · Measure · Mitigate

## A Guide for Prospective Clients

How we work, and how we can help.

This guide is for those  
considering an engagement.

It explains what protective  
intelligence is, why it matters,  
who we serve, where we look,  
and how an engagement  
actually works — before you  
decide to speak with us.



## BEFORE WE BEGIN

## A short orientation.

If you are reading this, you have most likely visited our website and want to understand, in more depth, what Aster Privacy actually does before deciding whether to speak with us. That is exactly what this guide is for. It is written plainly, and it answers the questions prospective clients most often ask — what protective intelligence is, why it matters, who we serve, where we look, when to engage, and how an engagement works in practice.

We work discreetly and by referral, with a small number of principals at any one time. Nothing in this document commits you to anything, and no enquiry obliges you to proceed. It is simply a considered explanation, so that any conversation we later have begins from a shared understanding.



## WHAT

## What protective intelligence is.

*Most people are familiar with cybersecurity, which protects systems, and with physical security, which protects people and places. Protective intelligence sits between them — and it protects the individual.*

Cybersecurity is largely concerned with defending an organisation's networks, devices, and data. Physical security is concerned with the safety of a person and their surroundings. Neither, on its own, answers a simpler and increasingly urgent question: **what is discoverable about you as an individual, and what could someone do with it?**

Protective intelligence answers that question. It is the discipline of finding what exists about a person across the internet — the visible web, the hidden and criminal web, and the regional platforms most tools never reach — understanding which of it is genuinely dangerous, and reducing it before it can be used against them. It is investigative and analytical rather than technical: the work is not to install software, but to see clearly, judge accurately, and advise plainly.

A digital exposure assessment — the core of what we do — is the practical form this takes. It is a structured examination of your exposure that results in a plain-language, risk-ranked account of what is out there, what it means, and what to do about it. Not a data dump, and not a vague reassurance: a considered picture, and a clear set of actions.

**IN SHORT** Protective intelligence protects the individual — mapping what is discoverable about you, judging what is exploitable, and reducing it before it becomes a real-world problem.



## WHY

## Why it matters — and why now.

*The most dangerous exposure is the exposure no one is looking at. By the time it feels like a threat, it has usually already been one for some time.*

For a person of standing — a principal, a founder, the member of a family office — a great deal of information exists online that was never deliberately made public. Home addresses sit in property and data-broker records. Routines and relationships can be inferred from the posts of others. Old credentials surface in breaches years after the fact. Individually, each fragment seems harmless. Assembled, they become something else entirely.

### How small exposures cascade

It is worth understanding, without alarm, how exposure actually escalates — because the chain is more connected than most people expect. Consider a single leaked password, of the kind that appears in ordinary data breaches:

— **It rarely stays contained.** Because most people reuse passwords, one leaked credential is quietly tested against many other accounts. A password exposed in a minor breach can open something far more important.

— **The email account is the master key.** If a reused password opens an email inbox, it opens almost everything else with it — because email is the reset mechanism for banking, finance, and government services. Access can be gained quietly, and the traces removed.

— **Identity enables impersonation.** Combined with a name and an identification number, that access allows a person to be convincingly impersonated — to a bank, a service provider, or a counterparty — opening the door to fraud and financial loss.

— **The digital becomes physical.** A name and an address, cross-referenced, reveal where someone lives. Combined with a routine inferred from public information, exposure that began as a line in a database can become a question of personal and family safety.

This is not offered to alarm, but to explain. None of these steps is exotic; each follows naturally from the one before. The point is simply this: exposure is rarely dangerous at the moment it appears. It becomes dangerous later — and quietly. That is precisely why it is worth seeing early.

## Why proactive, not reactive

Most people consider this kind of work only after something has gone wrong — an impersonation, a leak, a threat. By then, the exposure has usually existed for months, and the response is remedial rather than preventive. The value of protective intelligence lies in reversing that order: looking before there is an obvious reason to, so that exposure is found and reduced while it is still only exposure. The right time to look is before you feel the need to.

**IN SHORT** Exposure compounds quietly and is usually discovered late. Assessing it proactively — before an incident forces the issue — is the difference between prevention and damage control.

## WHO Who we serve — and who we are.

### Who we work with

Our clients share a common circumstance: their profile, wealth, or responsibilities make their personal exposure consequential in a way it is not for most people. In practice, they fall into three groups.

— **Private individuals.** Those who wish to understand what personal information about them is exposed, where they are visible across public and high-risk sources, and how to reduce privacy, impersonation, and reputational risk.

— **Founders and business owners.** Leaders whose personal and professional exposure are intertwined — where executive exposure, impersonation, or adverse online material can affect the individual, the business, or both.

— **Principals and family offices.** Those who require discreet, ongoing assessment and monitoring across public, high-risk, and region-specific environments — often including exposure linked to interests in China.

### Who we are

Aster Privacy is led by a founder whose career has been spent in the protection of people. That background began in uniform: as a Staff Sergeant and Close Protection Officer with the Singapore Armed Forces Military Police Command, planning and executing close-protection operations at a national level — an environment where the standard is exacting and the margin for error is small.

That grounding carried into the private sector, where the founder has spent years delivering executive protection for ultra-high-net-worth principals, both in Singapore and internationally — advancing venues and routes, leading threat assessments, coordinating protective operations under time pressure, and now leading a protection team as its Team Lead. It is work that trains a particular instinct: to anticipate a threat and reduce it quietly, before it ever reaches the person being protected.

What changed is where the threat begins. Increasingly, the route to a person starts not at their door but on a screen — in the exposure that precedes and enables real-world harm. Aster Privacy exists at the meeting point of these two

worlds: it brings the discipline of close protection to the digital domains where risk now originates. That dual vantage point — having stood beside principals in the physical world, and understanding how exposure is found and exploited in the digital one — is the whole point of the firm, and it is uncommon. It is also why our digital findings do not stop at the screen: we understand what they mean for a principal's physical security, because that is where the founder's work began.

**IN SHORT** We serve individuals whose exposure carries real consequence — and we approach it with the instincts of protection, earned beside principals in the field, not merely the tools of technology.

## W

### WHERE

## Where we look.

*A search engine reveals only a fraction of what exists online. The exposure that matters most often sits in the parts of the internet conventional tools never reach.*

Our work spans three domains. Together, they form a single picture of a person's exposure — and it is the combination, rather than any one of them, that makes the picture complete.

### The open web

The visible, searchable internet — but examined far more thoroughly than an ordinary search. Data-broker records, public filings, aggregated personal information, and the digital footprint assembled from public sources: the raw material from which a profile of a person is built.

### The dark web and high-risk sources

The hidden and criminal layers of the internet — breach databases, leak forums, paste sites, and marketplaces — where leaked credentials, exposed identifiers, and early indicators of impersonation or doxxing surface. This is where an exposure is often first traded, long before its consequences appear. We identify what is present and, where credible, validate it.

### Chinese-language and PRC-related platforms

This is the domain most conventional monitoring misses entirely. A vast, parallel internet — WeChat, Weibo, Douyin, Xiaohongshu and others — operates largely beyond the reach of Western search engines. For a principal with business, family, or reputational ties to China, a significant share of their exposure may live here, discussed on platforms their advisers cannot see and their existing tools cannot search. We work within these environments, in-language, to surface what would otherwise remain invisible.

### Where your information is held

Where matters in another sense too. Enquiries are received through secured channels and handled on a strict need-to-know basis. Any material an engagement produces is held securely, and personal data is retained only for as long as the engagement requires. The existence of an engagement itself may be treated as confidential by agreement.

**IN SHORT** We look across the open web, the dark web, and the Chinese-language internet — the last of which is, for many principals, the half of the picture no one else is examining.

## H

### HOW

## How an engagement works.

*Every engagement follows a deliberate sequence — Map, Measure, Mitigate — designed to move from a clear scope to validated findings to practical action.*

MAP

## We define scope and identifiers

We begin by agreeing what the engagement will examine — objectives, the identifiers in question, the languages and jurisdictions involved, and your preferences for escalation. Scope is confirmed in writing before any searching begins, including what we will not do. This discipline keeps the work lawful, proportionate, and focused entirely on what serves you.

MEASURE

## We search, monitor, and validate

We then assess your exposure across all three domains, and — crucially — separate signal from noise. Not everything discoverable is dangerous. Priority findings are validated rather than assumed, and we identify the credible pathways by which exposure could realistically be exploited. The result is judgment, not merely a list.

MITIGATE

## We deliver actions, and monitor if you wish

You receive a risk-ranked report written in plain language: what was found, what it means, and what to do about it, in what order. Where a finding carries physical-world implications, we say so. Where you want continued coverage, monitoring can be kept in place — keyed to your specific risk profile — so that if your exposure changes, you learn early rather than late.

### How an engagement can be structured

Most clients begin with a single assessment, and extend from there only where it is warranted. The lines below are advisory and tailored to the principal.

- **Assessment (core).** The foundational baseline of your exposure across all three domains, delivered as a risk-ranked report with clear, prioritised recommendations.
- **Remediation support (optional).** Turning recommendations into an execution plan — with clear owners, sequence, and verification that exposure has genuinely been reduced.
- **Ongoing monitoring (optional).** Continued vigilance keyed to agreed identifiers and thresholds, with early warning when your exposure materially changes.
- **Consultation — physical security (optional).** Advisory that extends protection from the screen into the physical world — described in full below.

**IN SHORT** You receive judgment and direction, not raw data — a clear account of what matters, why, and what to do about it, held in strict confidence throughout.

+

CONSULTATION

## Physical security, informed by intelligence.

*A digital finding rarely stays digital. An exposed address, a discoverable routine, a pattern of movement — each is a question of physical security as much as privacy.*

Because the founder's background is in close protection, Aster Privacy can do something few digital firms can: take what an assessment surfaces and advise on what it means for a principal's safety in the real world. This is offered as a distinct consultation line, drawn directly from operational executive-protection experience. It is advisory and assessment throughout — we assess, guide, and coordinate with your existing security providers rather than replacing them or installing anything ourselves.

### Residence and environment

Assessment of the home against what is discoverable about it — approach routes, sightlines, access points, and lighting — with guidance on address hardening, CCTV placement and coverage, access control, and, where wanted, secure-area planning. Specification and positioning advice; coordination with your chosen installer.

### Personal and executive protection

Guidance for principals who employ, or are considering, a close-protection detail — how to structure it, what competence looks like, and how to assess a provider — alongside secure travel and movement advisory that reduces the predictable pattern-of-life exposure a digital assessment so often reveals.

### Household and planning

Advisory on the security posture around domestic staff and family, and on how a household should respond to an incident — communications, escalation, and decision protocols — so a moment of pressure meets a plan rather than improvisation.

**IN SHORT** This is the clearest expression of what Aster Privacy is: protection for the principal across both domains — seeing the digital exposure, and understanding what it means in the physical world. It is the one thing a digital-only firm cannot offer.

**W****WHEN**

### When — and how — to begin.

The most useful time to assess your exposure is before there is an obvious reason to. Exposure found early is exposure that can be reduced quietly, on your terms, rather than addressed under pressure after an incident. If you are reading this, that time is most likely now — not because anything is necessarily wrong, but because you cannot act on what you have not yet seen.

Beginning is straightforward, and carries no obligation. A first conversation is simply that — a confidential, unhurried discussion of your situation and whether an engagement would serve you. There is no pressure, and no assumption that you will proceed.

### Begin a confidential conversation.

We work by referral and appointment. When you are ready, request a confidential call through [www.asterprivacy.com](https://www.asterprivacy.com). Enquiries are received only through our secured channels, and the existence of an engagement can be treated as confidential.

*Aster Privacy · Protective intelligence for principals · Singapore · By referral and appointment*