Privacy and intelligence services for those with the most to protect.

Digital Executive Protection

We identify exposure across your threat surface, reduce what can be weaponized through targeted removals and identity disruption, and maintain awareness through continuous threat monitoring.

Exposure creates risk.
Reducing exposure restores control.

The Stakes: Why It Matters Now

Every exposed data point can be a liability.

Home addresses, family connections, breach records, travel history, and identity fragments circulate across thousands of systems. An adversary only needs one.

For our clients, privacy is not a preference. It is operational security.

ObscureIQ's Digital Executive Protection program is built for high-risk individuals.

- Executives, founders, and board members
- Public figures and media personalities
- Investors and high-net-worth principals
- Families and teams facing elevated exposure

Those who need to control their exposure and stay ahead of emerging threats.

The Framework: *Map. Neutralize. Maintain.*

01: **Threat Surface Mapping**
Footprint audits reveal your full digital exposure across data brokers, the dark web, public records systems, and identity infrastructure. For most clients, the scale is unfamiliar. And clarifying.

02: **Deep Suppression**
Footprint Wipe and bespoke deletions remove traceable information across the broker ecosystem, including downstream aggregators most services never reach.

03: **Structural Identity Control**
Identity is not stored in one place. It is continuously reconstructed by brokers, public records systems, and identity graphs. We disrupt the links that let reconstruction happen.

04: **ThreatWatch: Active Threat Monitoring**
Continuous signal detection across social networks, dark web forums, paste sites, leak channels, and news platforms. AI aggregates. Analysts validate intent and escalate credible threats quickly.

Why ObscureIQ?

Built by intelligence and privacy professionals. Relied on by clients who cannot afford error.

We combine privacy operations with open-source intelligence to understand how exposure forms, spreads, and escalates. Most privacy services remove data. Most security tools scan for keywords. We analyze the full threat environment around an individual.

CODEX · 8,600+ Our internal dataset maps more than 8,600 organizations that collect, trade, or distribute identity data across the modern surveillance economy. It is the index behind every removal decision we make.

The Full Intelligence Picture

Our analysts study the complete exposure lifecycle:

- **Hostility Signals**: Narrative spikes, harassment patterns, and our internal Hostility Index.
- **Identity Infrastructure**: How identities propagate across brokers, records, and verification networks.
- **Exposure Pathways**: How leaks spread through forums, paste sites, social platforms, and broker networks .
- **Exposure Pathways**: We study how leaks spread through forums, paste sites, social networks, search engines, and data broker networks.
- **Breach Intelligence**: A repository of exposed credentials and leaked datasets circulating in underground communities.
- **Adversary Behavior**: How hostile actors gather intelligence, escalate, and move from online targeting to physical threat.

The ObscureIQ Equation:

Privacy operations + open-source intelligence.

Faster exposure reduction. Earlier threat detection. More precise response.

Schedule a Confidential Executive Briefing

Understand your exposure.
Reduce your risk.

ObscureIQ.com/coin 1-855-763-7273 Signal: PrivacyStan.10

Conversations are private and off-the-record by default.

We don't scan for words. We detect patterns, intent, proximity, and escalation.

ObscureIQ ThreatWatch

Early-warning intelligence for digital threats.
Built for those managing serious risk.

Threats rarely begin as attacks.
They begin as signals.

The Threat Landscape

Serious threats rarely begin with a visible attack.

They begin as fragments. Mentions in obscure forums. Signals buried in breach data. Early coordination inside closed communities. Individually, each fragment looks insignificant. Together, they form the early stages of real threat.

ThreatWatch detects and analyzes these signals as they emerge. This gives you visibility before response options narrow.

Three Layers of Detection :: Narrative. Chatter. Proximity.

01: Social & Narrative Signals

Social media, news, and the public web reviewed for targeting patterns, narrative spikes, and coordinated hostility. Custom threat tagging and analyst review surface escalation earlier than automated tools allow.

02: Dark Web & Fringe Threat Formation

Our proprietary OSINT system scans dark web, alt social, forums, fringe platforms, encrypted leak channels, paste sites, and hidden surfaces where hostile actors gather. NLP, AI, and human analysts combine to identify leaks and early threat signals others miss.

03: Digital Intent → Physical Movement

Some threats move from digital intent into physical space. Geofencing and location-targeted monitoring around homes, offices, and events detect when that transition begins. The moment visibility matters most.

Signals We Monitor

- Names, aliases, and usernames
- Organization or event names
- Bank account fragments, crypto wallets, leaked credentials
- Physical or digital addresses
- Unique identifiers and keyword patterns

Monitoring is passive, active, or near real-time, calibrated to your risk profile.

ThreatWatch detects patterns across vast data ecosystems.

Spectrum of Coverage

Our intelligence draws from the full digital ecosystem. These are representative. Full coverage is proprietary.

Video & Image Hosting
YouTube, Twitch, Vimeo, Imgur, Flickr, Dailymotion

Messaging Platforms
Telegram, Discord

Alt Social Platforms
Gab, Truth Social, Rumble, VK, Bluesky, Mastodon

Forums & Pastebins
4chan, 8kun, Incels.is, chan boards, 72 pastebins

Blogs & News Sites

Mainstream Platforms
Twitter/X, Facebook, Insta, LinkedIn, Reddit, TikTok

The Method

AI aggregates and ranks signals. Analysts review, investigate, and validate intent.

Automation alone misses the patterns that matter. Analysts alone cannot cover the surface. ThreatWatch pairs them: machine scale with human judgment.

Schedule a Confidential Briefing

Early visibility. Measured response.

ThreatWatch

ObscureIQ.com/coin | 1-855-763-7273 | Signal: PrivacyStan.10