

ACCOUNTABLE LICENSE-PLATE INTELLIGENCE, EXPLAINED FOR THE PUBLIC.

This document explains, in plain language, what TRAICE is, how it works, and what it will never do. It is written for residents, councils, and community groups — not for police departments. Everything in it is a design fact about the software, not a marketing promise.

WHAT TRAICE IS

TRAICE is **investigative software for police departments**. It works with license-plate-reading cameras a town already owns, and detectives use it to solve real cases — burglaries, stolen vehicles, hit-and-runs, missing people. TRAICE is not a camera network: it does not own cameras, does not own data, and never pools information between towns. The department owns everything; TRAICE licenses only the software.

THE PROBLEM IT ANSWERS

License-plate readers are spreading fast, and in most deployments the public has no way to know **who searches the data, why, or how often**. Access is governed by policy binders, not by the software itself — and audits and reporting around the country have repeatedly found casual lookups, personal-purpose searches, and data shared far beyond what communities were told. The technology is not the problem. Unaccountable access is.

HOW A SEARCH ACTUALLY WORKS IN TRAICE

1

A documented case comes first.

A search cannot exist on its own. It must be attached to a real investigation with a case number.

2

A written reason, in advance.

The officer states why the search is needed. Thin, vague, or personal-sounding reasons are automatically routed to a supervisor.

3

The policy engine decides — not the officer, not the AI.

Deterministic rules block overbroad sweeps before they run: limits on radius, time window, and scope are enforced by code.

4

A signature, and approval where required.

The officer certifies the request under their own name. Searches that need a supervisor do not run until one approves — and no one can approve their own request without a recorded attestation.

5

A permanent record.

Every step lands on a tamper-evident, cryptographically chained audit log. There is no delete button — for anyone. Every 30 days the entire dataset is frozen into an immutable, downloadable version.

WHAT THE CAMERAS DO — AND DON'T

The cameras photograph **license plates and vehicles**. TRAICE does not use facial recognition and does not identify people from images. The system's founding commitments, in writing in every agency agreement: the department owns all hardware and data outright; data is never sold or monetized; data is never pooled into a regional or national network; and no capability is added that turns plate reading into people tracking.

THE PUBLIC PORTAL — CHECK YOUR OWN PLATE

Agencies running TRAICE expose a public portal where anyone can enter a plate and see when a **person** — not a camera — accessed it: inclusion in an authorized search's results, a match against an agency alert list, or a profile opened by personnel. Machine scans don't appear; human access does.

Two deliberate limits, explained rather than hidden: the portal never shows locations — a public map of sightings would let anyone track any car, including an abuser tracking a victim. And events appear after a disclosure delay (typically 90 days), so an active investigation is never tipped off to the person being investigated. You still get the truth; transparency just doesn't become a lookout service. Every public check is itself recorded — every search leaves a trace, including yours.

STRAIGHT ANSWERS TO FAIR QUESTIONS

Is TRAICE certified? No certifications are claimed. The platform is designed to align with CJIS security standards and is validated with each agency and its state authority during onboarding.

Does this cover every camera in my town? No. The portal only reflects agencies running TRAICE. It cannot see — and does not excuse — any other system a town may operate.

Who is behind this? TRAICE is a new, independent company. We would rather tell you that plainly than pretend otherwise — the entire product is built on the idea that trust is proven, not asserted.

What should a resident do with this? If your town is debating license-plate readers — or regretting them — the question to bring to your council is not "cameras or no cameras." It is **"secret access or accountable access."** Ask whether your town's current system can show you, the public, when a person searched a plate. If it can't, ask why not.

For councils and community groups: we will put every claim in this document in writing for your town, walk any group through a live demonstration on synthetic data, and answer any question on the record. Reach us at info@traicesafety.com.