FIELD BRIEFING · 001

The AI Era Does Not Just Capture Attention. It Captures Cognition.

A field briefing on AI surveillance, inference, and the new geopolitics of data.

BEGIN →

THE FRAME

Every AI app collects.
The real questions are sharper.

- **What** are they collecting?
- **Who** gets access to it?
- **How long** is it stored?
- Can it be **linked back** to you?
- Can it be **weaponized** later?

01 · THE MODEL

Surveillance-for-convenience is the default operating mode.

It is not limited to chatbots. It runs across:

- Keyboards, browsers, meeting assistants
- Productivity tools and AI note-takers
- Smart glasses and voice assistants
- AI photo editors and image apps
- Companion apps and so-called AI girlfriends

02 · INPUTS

What AI apps can collect.

- Conversations and prompts
- Voice recordings
- Uploaded documents
- Contact lists and calendars
- Photos and metadata
- Screen activity
- Clipboard contents
- Location data
- Browsing behavior
- Device identifiers
- Typing patterns and cadence
- Biometric: voiceprints, face
- Behavioral profiling signals
- Cross-app correlation traces

03 · HIGHER-ORDER SIGNALS

Some systems also collect what you never explicitly share.

- Emotional patterns
- Political leanings
- Purchasing intent
- Relationship dynamics
- Personal vulnerabilities
- Psychological traits

Commercially valuable. Strategically valuable.

04 · THE REAL RISK

The danger is not collection. It is inference.

An advanced AI system can infer whether you are:

- Stressed or financially unstable
- Lonely or politically persuadable
- Likely to resign from your job
- Vulnerable to scams or addiction
- Planning travel or preparing litigation
- In active conflict with someone

Without you ever saying it out loud.

05 · FORCE MULTIPLIER

Inference becomes power when combined with everything else.

Pair AI inference with:

- Ad-tech and social-media tracking
- Financial systems and telecom metadata
- Cloud providers and SaaS workflows
- Insurance and employment pipelines
- Government and platform access requests

06 · WHO IS ACTUALLY LISTENING

Mostly machines.
Sometimes humans.

The default is automated collection, analysis, and profiling.
Documented cases also include:

- Contractors reviewing voice recordings
- Employees accessing private user data
- Training datasets exposing sensitive content
- Governments demanding platform access
- Breaches leaking AI conversation histories

Centralized data collection always creates risk.

07 · GEOPOLITICS

AI is becoming national infrastructure.

Countries treat AI data as intelligence, economic, and behavioral-control assets. Expect:

- AI sovereignty laws and localized stacks
- Stricter data-residency requirements
- Offensive AI espionage operations
- AI supply-chain conflicts
- Synthetic influence and cognitive warfare

The future conflict space is behavioral dominance at population scale.

08 · ARCHITECTURE

Open source vs closed AI. Trust is the real currency.

- Open-source models can run locally and be inspected
- But many open apps still phone home
- Most users cannot actually audit code
- Local models can leak through plugins and telemetry
- Closed systems are convenient but require trust

09 · OPERATIONAL POSTURE

If you work in high-risk fields, assume exposure.

Journalism · cybersecurity · investigations · law · diplomacy · activism · defense · intelligence · crisis · corporate strategy.

- Prompts may eventually become discoverable
- Uploaded files may not stay private forever
- Metadata matters as much as content
- Adversaries may target your AI workflows

Treat AI as a semi-trusted external analyst in the room.

Not a priest hearing confession.

10 · COUNTERMEASURES

Five practices for serious operators.

01 **Segment your AI usage**
Separate tools for casual, sensitive, research, and personal contexts. Never centralize your whole cognitive footprint.

02 **Do not upload raw sensitive data**
No passports, client lists, unreleased investigations, legal strategy, crisis data, or credentials. Sanitize first.

03 **Use local AI for high-sensitivity work**
Ollama, LM Studio, AnythingLLM. Offline transcription. Self-hosted vector databases.

04 **Audit permissions aggressively**
Microphone, photos, Bluetooth, contacts, background refresh, accessibility. Most users massively over-permission.

05 **Assume breach eventually**
Logs may leak. Insiders may exist. Laws may change. Design for that reality, not the marketing copy.

11 · THE SHIFT

The internet era captured attention.

The AI era captures cognition.

AI systems may soon know what humans say, what they think, what they fear, and what they are likely to do next.

That changes privacy, politics, warfare, relationships, commerce, and human autonomy itself.

Threat intelligence
for the cognition era.

If this was useful, repost it for the operator,
analyst, or executive in your network.

Follow BLK CORAL INTELLIGENCE
for field briefings on AI, security, and behavioral risk.

www.drmalvikamehta.com

END OF BRIEFING