

WHERE DIGITAL EVIDENCE LIVES

i Treat the whole scene as a **network of recorders** — the home, the person, the vehicle, and the cloud each capture location, time, and activity.

A NETWORK OF RECORDERS



Home

+



Person

+



Vehicle

+



Cloud



LOCATION · TIME · ACTIVITY

HOME / NETWORK

- **Doorbell & security cameras** — video, motion events, clips
- **Smart speakers & hubs** — voice, wake events, logs
- **Router / DVR / NAS** — connections, MAC addresses, logs
- **Smart TVs & streaming** — watch & casting history
- **Smart locks / thermostats** — entry & automation logs
- Computers, tablets, printers, game consoles

PERSON: PHONE & WEARABLE

- **Phone** — calls, texts, apps, media, location
- **Smartwatch / fitness tracker** — activity, health, location
- **Earbuds & Bluetooth accessories** — connections, usage
- **SIM / eSIM** — carrier data, subscriber identifiers
- Laptops, tablets, backup & storage media

VEHICLE

- **EDR / airbag control module** — crash & event data
- **Infotainment** — paired phones, contacts, navigation
- **Dashcam** — video, audio, GPS, impact clips
- **Telematics / OBD** — location, driving behavior
- **Key fob / remote-start app** — lock, start, proximity

CLOUD — ACCOUNTS, LOCATION, MESSAGES, BACKUPS

- Email, social media, photos, files, and app data
- Service-provider logs and account records
- Content often **survives even after local deletion**
- Accounts **corroborate** device data across sources

HANDLING PRINCIPLES

- **Think beyond the device** — data lives in many places and correlates
- **Time is critical** — synchronize and preserve it
- **Preserve the state** — never explore or alter the device
- **Document everything** — what you see, what you do, and when


KEY TAKEAWAY

Phones, wearables, vehicles, homes, and the cloud **corroborate one another** — and a seized cell phone still requires a **warrant to search** (*Riley v. California*).

NETWORK OF RECORDERS

PRESERVE THE STATE

WARRANT TO SEARCH

