Ghost Mode Strategies
Counter-Surveillance and Detection for People Like Us

We are being watched.

Our data has been exposed.

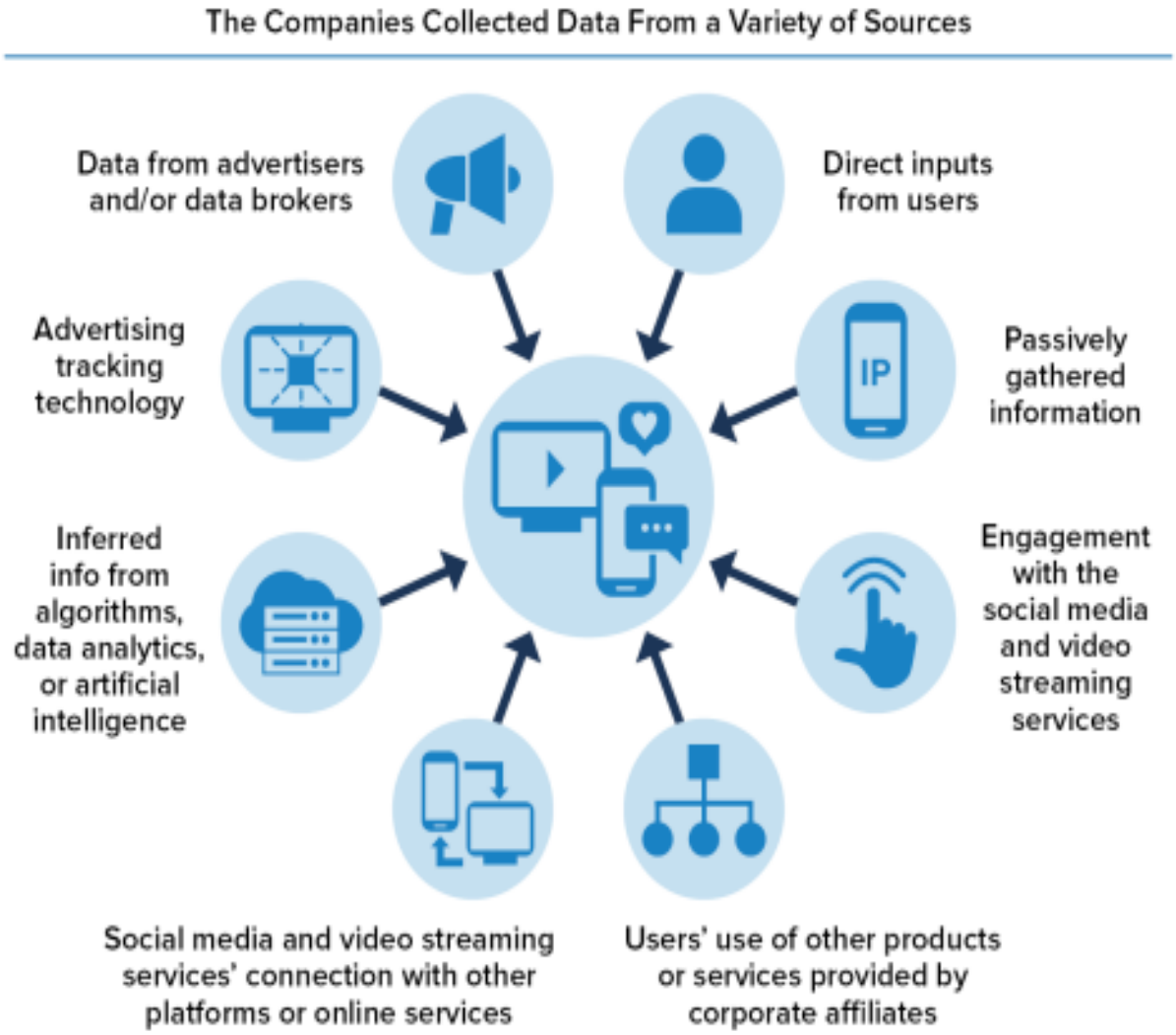
Doxxing is real.

Our homes are bugged, along with our fuel-efficient and environmentally friendly vehicles.

We are the reality stars in our show, without the compensation and all the manipulation

Exploring counter-surveillance tools and technologies for effectiveness

Data category	Type of data
Contact info	Name
	Email address
	Phone Number
	Physical address
	Other user contact info
Health and fitness	Health
	Fitness
Financial info	Payment info
	Credit info
	Other financial info
Location	Precise location
	Coarse location
Sensitive info	Sensitive info
Contacts	Contacts
User content	Emails or messages
	Photos or videos
	Audio data
	Gameplay content
	Customer support
	Other user content
Browsing history	Browsing history
Search history	Search history
Identifiers	User ID
	Device ID
Purchase history	Purchase history
Usage data	Product interaction
	Advertising data
	Other usage data
Diagnostics	Crash data
	Performance data
	Other diagnostic data
Surroundings	Environment scanning
Body	Hand movements
	Head movement
Other types of data	Other data types





Data That Tesla Collects From Customers

Data collected from users and their devices
- Name
- Address
- Phone Number

Data collected during vehicle services
- Customers name
- Vehicle identification number
- Repair history

Data collected through credit applications and other forms
- Driver's License
- Date of birth
- Social Security Numbers
- Bank routing information

Data collected offline
- When a customer has visited a tesla store or repair facility
- Attended a Tesla event
- Signed up for a test drive

Data collected from browser or device
- Media Access control access
- Computer type (windows/Mac)
- Language

Data collected from tesla vehicles
- Speed Information
- Odometer Readings
- Camera Images

Personal information in the vehicle that Tesla can access
- Contacts
- Browsing history
- Navigation history

Data collected from Tesla energy products
- Information about home
- Dimensions of roof
- Configuration of electrical systems

Smart Home



Camera



Light



Smoke Alarm



Smart TV



Washing Machine



Smart House



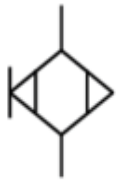
Motion Sensor



Thermostat



Refrigirator



Moisture Sensor



Lock



OpenClose Sensor



Doorbells

Innovative Techniques for Mobile Counter-Surveillance

1

Passive Surveillance

Credential and Data Leaks
Exposure opportunities
Reconnaissance

2

Surveillance often starts from Publically Available Data

3

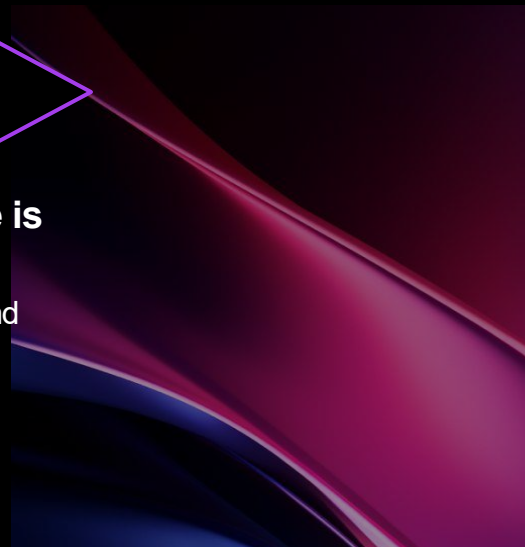
Understanding surveillance is Not Always Obvious

Exposed IPs, Metadata Leaks and Social Media

4

Protecting our Data is not Enough - Proactive Detection

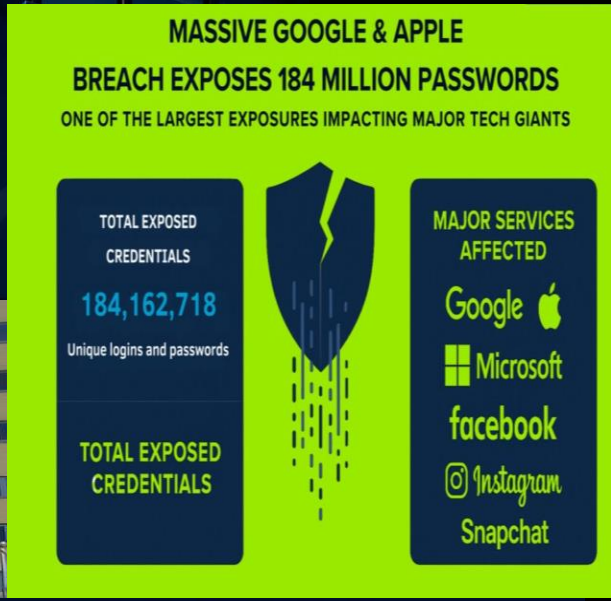
Let's even the playing field using open-source intelligence counter-surveillance giving you access and visibility from from anywhere and everywhere.



Let’s take a quick peek at the current data exposure climate











DATA COLLECTION ON CONSUMERS

SINCE DECADES



Public available data, court records, vehicle records, voter records



Name and address changes, marriages, divorces, births, deaths



Lists from surveys, warranty registrations, and sweepstakes



Newspaper and magazine subscribers, mailorder buyers, travel bookers



Purchases from retailers, pharmacies, loyalty programs, clubs



Credit histories, data from banks, credit card networks, insurers, healthcare, employers

Name

Birthdate

LINKING

Postal Address

Phone ZIP

CENSUS DATA, MARKET RESEARCH

DATA ABOUT NEIGBORHOODS & BUILDINGS

HOUSEHOLD-LEVEL DATA

INDIVIDUAL-LEVEL DATA

UNIQUE IDENTIFIERS

YOUR PROFILE

Family

Interests

Attitudes Lifestyle

Financial Health

Behaviors Personality

Risk Factors

Weaknesses

Movements

Retailer

App

Publisher

Data broker

Credit card network

Data broker

App

Loyalty programm

Insurer

Social network

Bank

Profile data is stored by many companies from retailers to data brokers to online platforms.

RECENT YEARS

AGGREGATED, ANONYMIZED "BIG DATA"

METADATA ABOUT WEB-SITES, APPS, CONTENT, PLACES

BROWSER OR DEVICE SPECIFIC DATA

INDIVIDUAL-LEVEL DATA

UNIQUE IDENTIFIERS



Publicly available data on the web



Website visits, searches and other behaviors



Social media, platforms and user accounts



Smartphone and app usage



Online Purchases



Smart TVs, activity trackers, game consoles, e-readers, cars and other devices

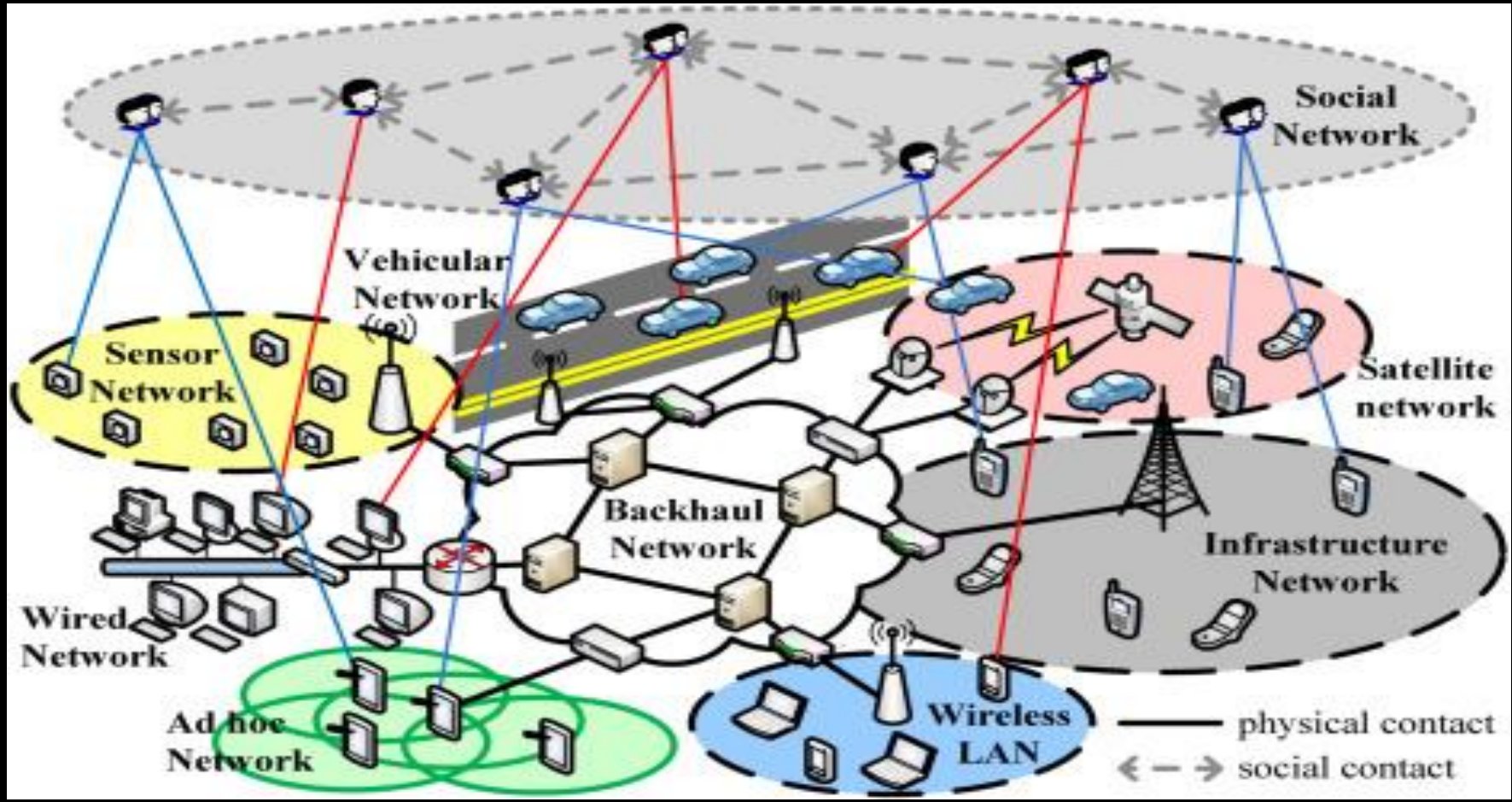
Location

Device IDs

LINKING

Accounts Email

Cookie IDs


Social Network
Vehicular Network
Sensor Network
Satellite network
Backhaul Network
Infrastructure Network
Wired Network
Ad hoc Network
Wireless LAN
physical contact
social contact

Strategies for OSINT Defense



Identifying common surveillance tactics

Learn to recognize the most prevalent surveillance methods used by adversaries to effectively counter them.



Community insights on counter-surveillance

Using their methods to detect our own exposure



Methodologies for neutralizing threats

Develop proactive strategies and methodologies for neutralizing identified surveillance threats before they escalate.

Leveraging OSINT for effective counter-surveillance practices

1

Integrating OSINT into surveillance strategies

Utilize open-source intelligence (OSINT) to enhance situational awareness and counter-surveillance strategies effectively.

2

OSINT tools for surveillance detection

Explore various OSINT tools that can assist in identifying and mitigating surveillance threats in real-time.

3

OSINT tool development

Connect with experts in the OSINT field to share knowledge and strategies for counter-surveillance practices.

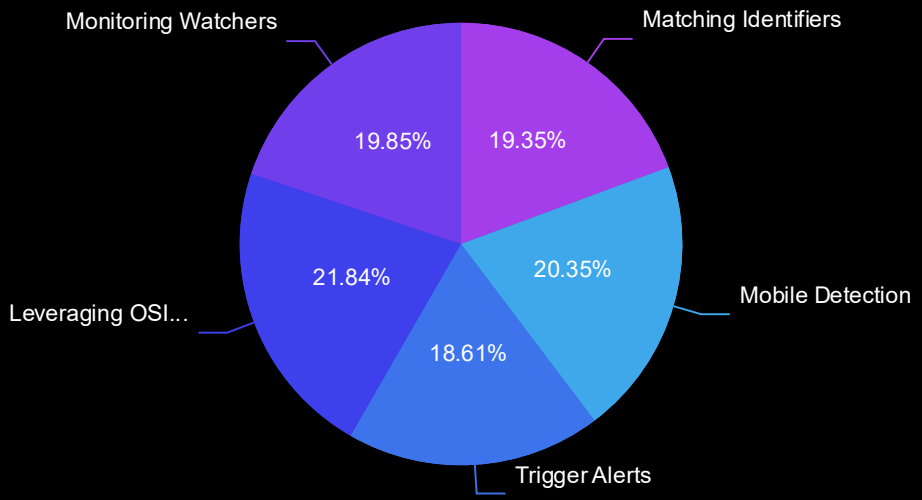
4

Best practices for OSINT utilization

Implement best practices for gathering and analyzing OSINT data to enhance your overall counter-surveillance strategy.

How Ghost Mode Works





Personal Counter-Surveillance Recipe

2 Understanding the role of OSINT in enhancing surveillance awareness

TOOLS to Build Freely

- Python scripts and open-source
- OSINT tools: Shodan API & BeautifulSoup
- Alerting: Signal CLI & Telegram Bot
- Mobile Phone (no laptop required)
- Options: Tor-Over-VPN, Raspberry Pi+ power bank (global and portable)



Maximizing OSINT Usage to Identify Hidden Surveillance



1

Effective Techniques for OSINT Analysis

Utilizing various OSINT tools can greatly enhance your ability to detect hidden surveillance methods and devices around you.

2

Identifying Patterns in Surveillance

By analyzing public data sources, you can identify patterns of surveillance that enable you to anticipate potential watchful eyes.

3

Community Engagement in Counter-Surveillance

Engaging with local communities can provide insights into suspicious activities and enhance overall vigilance against watchful observers.

Methods for utilizing OSINT in counter-surveillance efforts

Gathering Publicly Available Information

Collecting information from public records and online resources can significantly aid in identifying those conducting surveillance.

Utilizing Geospatial Intelligence

Geospatial data can reveal unusual patterns of movement or gathering, alerting you to potential surveillance efforts.

Best practices for watching the watchers effectively

Maintaining a Low Profile

Adopting a low-profile approach can prevent surveillance efforts from identifying you as a counter-surveillance target.

Utilizing Surveillance Detection Routes

Creating and practicing surveillance detection routes can help you spot any potential watchers on your tail.

Developing Situational Awareness Skills

Improving your situational awareness can make you more adept at spotting suspicious behavior or hidden surveillance.

Regularly Reviewing Surveillance Techniques

Stay updated on the latest surveillance technologies and tactics to better prepare for counter-surveillance.

Ghost Mode - Use Cases



- Set up **honeypot infrastructure** and fake IDs (email, domain).
- Run Ghost Mode to monitor OSINT sources for those identifiers.
- Log first-seen data points and respond with **automated takedown** workflows.
- Install Ghost Mode on **Termux (Android)** or a **Kali Live USB**.
- Scan for SSIDs, IP exposure via Shodan, and username mentions online.
- Receive alerts on a pre-configured **Telegram bot**
- Boot Ghost Mode from a **USB with Tails OS**
- Monitor for name, username, and metadata online.
- Set up **air-gapped alerts** via Tor + Signal CLI for covert notification.

Go Ghost Mode. Stay Free.

Surveillance is real. Ghost Mode is the counter to the global consumption of your private data.

OSINT solutions are available to protect and secure your information from unwanted access everywhere.

Thank You

Désirée Michelle W.