OSINT Enabled Ghost Mode: Counter-Surveillance for Everyday People Like Us

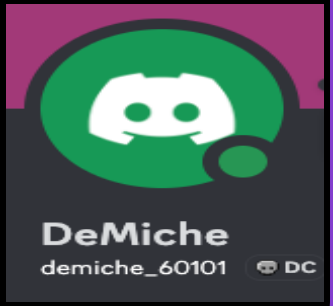
whoami

Désirée Michelle

- Over 15 years in Information Security
- Founder of Quantum Mergers
- Experienced with Fortune 500, DoD, Financial, Health Telecommunications, and the Energy Sector
- Forbes Business Council Member, Contributor to OWASP, CSA, and the Global Business Resilience Council
- I solve security problems for a living, I am an architect and a creator and this is my playground.

contact

- Discord: DeMiche
- LI: https://www.linkedin.com/in/desiree-wilson-cissp-gcih/
- Github : https://github.com/desimic



We are being watched!

Our data has been exposed.

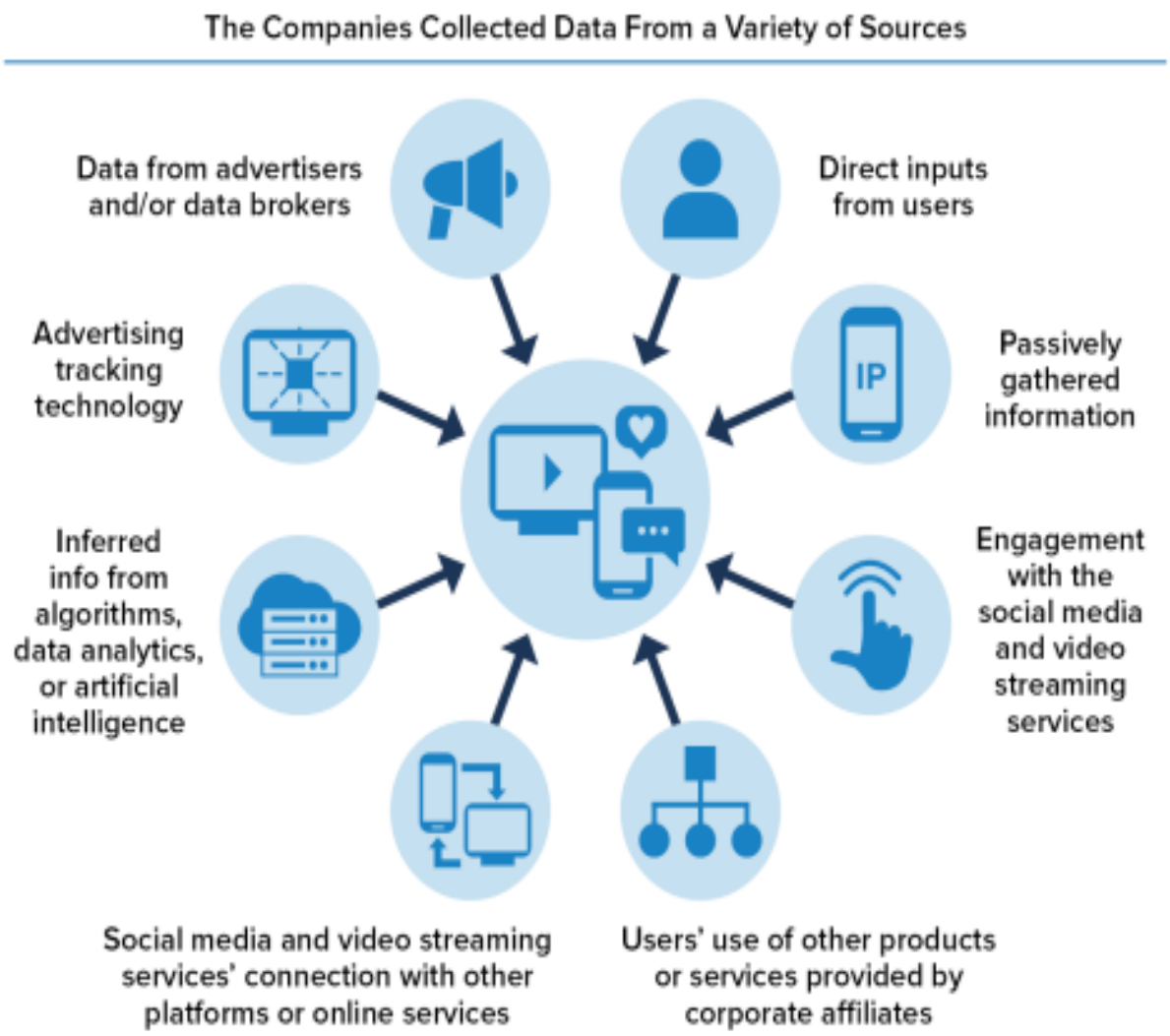
Doxxing is real.

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

Today we explore OSINT counter-surveillance tools and technics to flip the script and watch the watchers

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



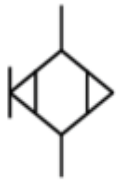
Motion Sensor



Thermostat



Refrigirator



Moisture Sensor



Lock



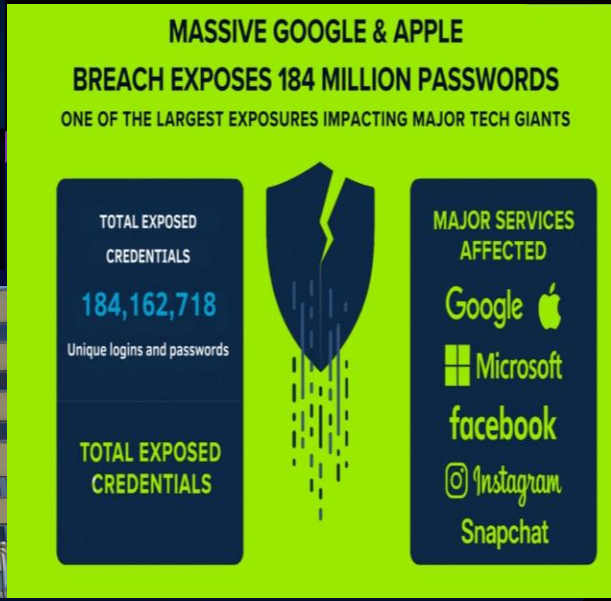
OpenClose Sensor



Doorbells

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

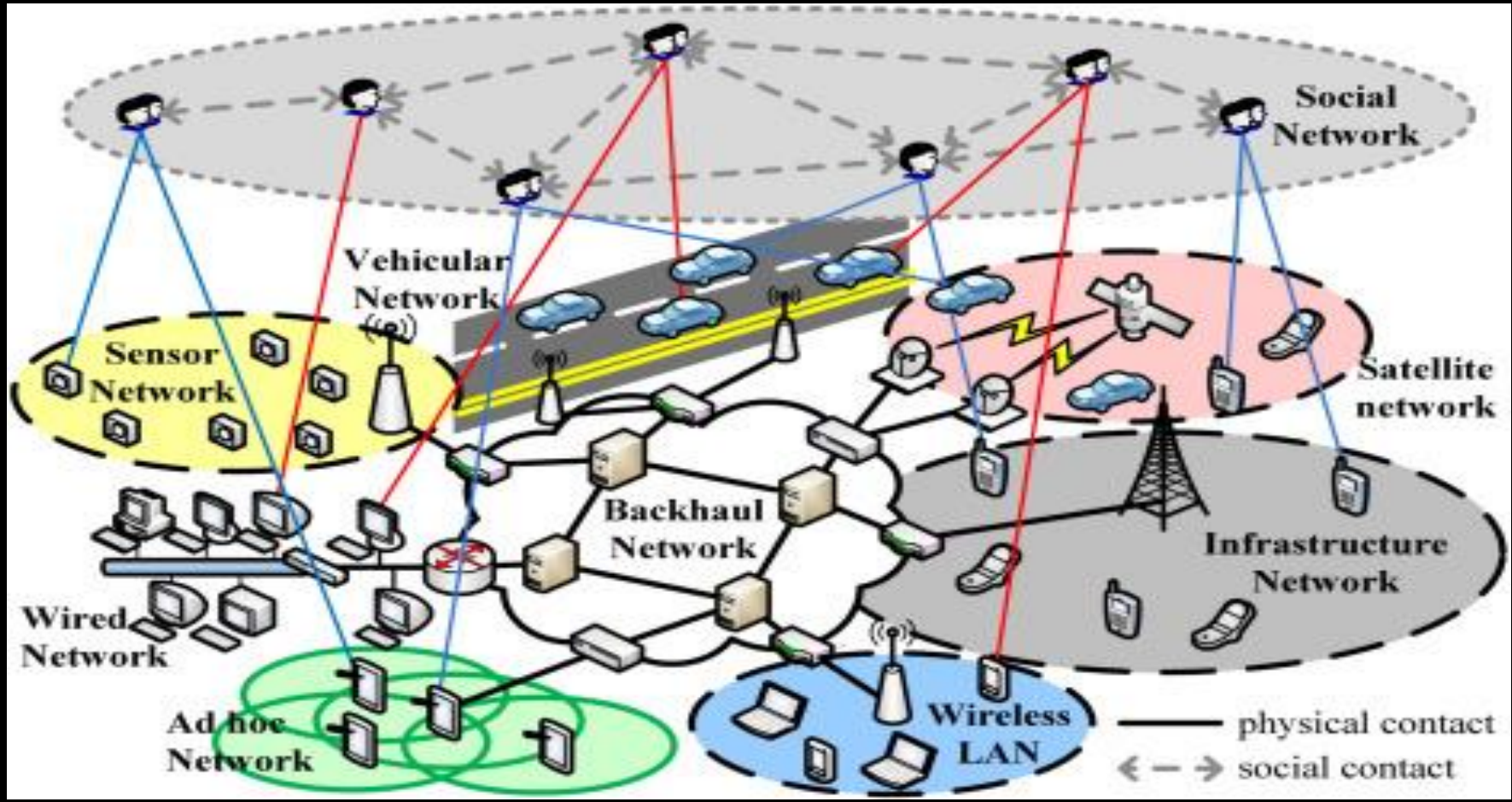
Location

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

Innovative Tools for Mobile Counter-Surveillance

Surveillance often starts from Publically Available Data

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.

1

2

3

4

Passive Surveillance

Credential and Data Leaks
Exposure opportunities
Reconnaissance

Understanding surveillance is Not Always Obvious

Exposed IPs, Metadata Leaks, and Social Media




Go GHOST Mode

Strategies for OSINT Defense



My Personal Counter-Surveillance Recipe

SpiderFoot - OSINT scanner
Ntfy - push notifications



Watch Safely

Tailscale - private global access
OpenCanary - honeypot system
Canary Watch - real time watcher



Bring it all together

Docker - self host

All Containers are Running - Test Mobile – Counter-Surveillance on the Go



- Tailscale
- ntfy
- SpiderFoot
- OpenCanary
- Canary+Watcher
- Dashboard

- https://github.com/desimic/osint_surveillance_detector_repo

GHOST MODE: A system designed to detect surveillance while preserving mobility, privacy, and security.

ALERTS

NTFY - Shows if alert scripts are running – push messages

- Dashboard UI for recent activity logs

SpiderFoot

Performs an automated search of your designated scan items

OpenCanary

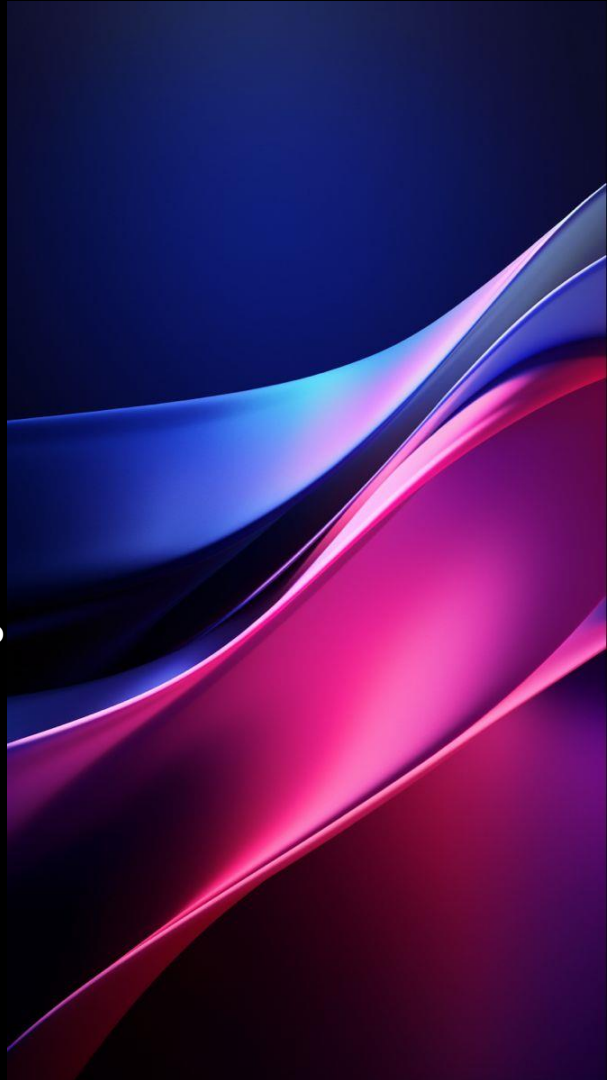
Shows trap events when someone probes your fake services

Canary+Watcher

Shows when it parses opencanary.log and pushes to ntfy

How Ghost Mode Works!

- Alert Handling
- When you receive an alert ntfy pushes alerts to your UI Dashboard
- The dashboard contains your activity log
  OpenCanary HoneyPot Traps – Watcher wired to ntfy, enabling all alerts to appear in the dashboard log
- Tailscale + MagicDNS for Private Global Access
- If a threat is confirmed – isolate the device, rotate credentials, check logs, continue to be diligent in surveilling the threat. Now you are watching them!



Understanding the role of OSINT in enhancing surveillance awareness

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.

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

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

Time-Based Monitoring

Track the timing and frequency of suspicious activity to detect patterns, like coordinated movements or surveillance cycles.

Methods for utilizing OSINT in counter-surveillance efforts

Analyze information from Different OSINT Sources

Establish a baseline for detecting anomalies, use various sources and assets to connect scattered pieces of intelligence and build a picture over time so you can recognize anomalies

Utilizing Geospatial Intelligence

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

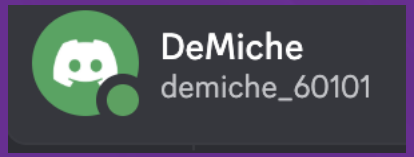
Go Ghost Mode.

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

GitHub Repo:

https://github.com/desimic/osint_surveillance_detector_repo

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



Thank You

Désirée Michelle

