ADVERTISING INTELLIGENCE AND OTHER WAYS TO LOCATE PEOPLE VIA MOBILE PHONES

Igor Bederov

Chair, Council for Countering Technology-Related Offenses
Coordination Council of Russia's Non-State Security Sector

Internet-Rozysk (part of the CYBERSYSTEM Group)



LET'S GET ACQUAINTED!

Russian businessman and public figure. Founder of the Russian company Internet-Rozysk, inventor and advocate for the adoption of innovation in law enforcement. Creator of analytical products and methods for preventing and investigating information and telecommunications crimes.

> "The Sherlock Holmes of the digital age" - RUBEZH magazine

- Chair, Council for Countering Technology-Related Offenses, CC of Russia's Non-State Security Sector
- Member of the expert council of the International Corporate Security Association (ICSA)
- Adviser to the Governor of Vladimir Region
- Adviser to the Governor of Vologda Region
- Assistant to a senator of the Russian Federation
- Expert at the SafeNet Engineering Center, National Technology Initiative (NTI) 20.35
- Board member, St. Petersburg Federation of Competitive Programming
- Co-founder of the SB-Piter club of security executives
- Founder of Internet-Rozysk (part of the Cybersystem Group)





IGOR BEDEROV

THE EVOLUTION OF LOCATION FINDING IN GSM NETWORKS

From broad coverage areas to precise coordinates

MOBILE NETWORK ARCHITECTURE (2010s)

MOBILE PHONE

BASE STATION (BTS)

NETWORK CONTROLLER (BSC)

SHORT MESSAGE SERVICE CENTER (SMSC)

TELECOMMUNICATIONS INFRASTRUCTURE

--- RADIO SIGNAL

--- CONTROL

--- DATA TRANSFER

ANDROID DEVICE MANAGEMENT

APPLE DEVICE ECOSYSTEM

AUTHENTICATION: THE KEY TO DEVICE CONTROL

Email: user@example.com

Password: ••••••••••

DEVICE ACCESS



GSM NETWORK GEOLOCATION



LOCATION REFINEMENT PROCESS

BROAD AREA → BASE STATION SECTOR → CELL (200-1,000 m) → APPROXIMATE LOCATION

EVOLUTION OF GEOLOCATION TECHNOLOGIES

1. HISTORICAL METHODS

Manual area location

- Imprecise data

2. CELL IDENTIFIERS

Cell ID (CID)

LAC / MCC / MNC

Link to a base station

3. COVERAGE MAPPING

Coverage databases

Signal propagation models

4. APPROXIMATE LOCATION FINDING

Triangulation

Signal strength

Antenna sector

Error margin: 100s of meters to km

5. MODERN POSITIONING METHODS

GNSS (GPS/GLONASS)

+ A-GPS, Wi-Fi, BLE

High accuracy (meters)

MAIN SOURCES OF LOCATION DATA

BASE STATIONS GSM

SIGNAL STRENGTH

ANTENNA SECTOR

COVERAGE DENSITY

SATELLITE NAVIGATION SYSTEMS

IMPROVEMENTS IN LOCATION ACCURACY

2G / GSM (2000s)	3G / UMTS (2010s)	4G / LTE (from 2015)	5G / NR (2020s)	GNSS + AI (TODAY)
100 m - 10 km	50 m - 1 km	5 m - 100 m	1 m - 10 m	<= 1 m

ACCURACY: LOW → HIGH

KEY DEVELOPMENT MILESTONES

1991	1997	2001	2007	2012	2016	2020+
GSM network launch	Introduction of LBS services	A-GPS in mobile phones	Smartphones and mapping services	Wi-Fi / A-GPS widespread use	VoLTE, NB-IoT positioning	5G, AI, RTK centimeter accuracy

TRACKING A MOBILE DEVICE



Determining a mobile device's location is one of the most common tasks in an OSINT specialist's work.

Reasons range from finding a relative's lost phone to testing hypotheses during an investigation.

All methods require a lawful basis for their use and a thorough understanding of ethical standards.
Unauthorized surveillance is a criminal offense.

MOBILE DEVICE TRACKING METHODS FALL INTO TWO CATEGORIES:

WITHOUT ACCESS TO THE DEVICE

Methods that obtain a device's location remotely, without physical interaction with it.

VS

WITH ACCESS TO THE DEVICE

Methods that require an unlocked device to install tools, change settings or extract data.

All actions must comply with the law and ethical standards.
Unauthorized surveillance is a criminal offense.

WHEN ACCESS TO THE PHONE IS POSSIBLE

1 PARENTAL CONTROL SOFTWARE

After a one-time physical installation and setup on the target device, the app provides remote access to its data.

- Real-time location
- Movement history
- Messages and messengers
- Calls and contacts
- Other data



- Runs discreetly
- 24/7 monitoring
- Data in the cloud
- Instant notifications

Originally designed to protect children, it can monitor adults with their consent and within the law.

2 MOBILE CARRIER SERVICES

Standard paid services from mobile carriers, such as Locator or Geosearch.

MTS · Beeline · MegaFon · TELE2

Location-finding technologies

LBS (Location-based service)
Location based on carrier network data

Triangulation
Location based on signals between cell towers



- High accuracy
- No software installation
- Legal via the carrier

Accuracy depends on network coverage density and may reach 10-100 meters in urban areas.

3 LIVE LOCATION SHARING

Enabling "Share location" in popular messengers and mapping services.

Telegram · Google Maps · Other services

Select contact → Enable location → Select duration → Transmit coordinates



- Real time
- Access control (who and for how long)
- Transparent to the user

Works only with the device owner's consent.
Simple, quick and convenient.

LOCATION ACCESS REQUIRES PHYSICAL ACCESS TO THE DEVICE OR THE OWNER'S CONSENT.
Use only lawful methods and respect privacy.



For an OSINT specialist, a locked smartphone is not a dead end, but a challenge.

Investigations where information on a phone is critically important (from preventing crime to finding missing people) require skills to bypass its protection.

The lock screen does more than restrict access: it blocks key functions.

Yet technology often gives way to psychology.

WARNING: Unauthorized access to devices is punishable by law.

ACCESS METHODS: HUMAN FACTORS AND TECHNIQUES

- 70% of owners willingly share the code, especially if it speeds up the device's return.
- Seizing the phone physically at the moment it is unlocked.
  Asking to "make a call" works in a similar way.
- Watching the code being entered, in person or through CCTV.
- Looking for notes in notebooks, under the case, in the cloud or in leaks.
  20 combinations account for 26.83% of passwords (1234, 1111, 0000).
  Simple geometric patterns (letters, angles) are guessed in the first few attempts.
- Dusting the screen with powder (even baby powder) reveals finger marks.
  Analyzing the marks and the owner's habits narrows down the possibilities.
- A 3D fingerprint replica or face mask (a photo on a 5-liter jar) can fool biometrics.
  Older scanners are vulnerable to photos. Modern ones (Face ID, ultrasonic sensors) are harder to fool, but not invulnerable.

ACCESS VIA A SIM CARD IN AN UNLOCKED DEVICE



1. Physically remove the SIM card from the locked device.
2. Make sure the SIM is not PIN-protected.
3. Insert the SIM into an unlocked smartphone with a clean OS.
4. Enable mobile data and recover access to the required accounts using the "Forgot password?" feature.
5. You can download GSM connection records from your carrier's account portal.
6. Movement history is available through Android or iOS services.

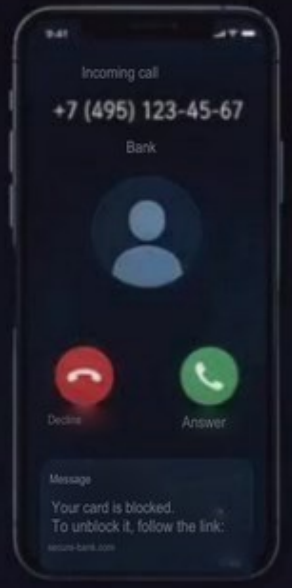
Law and ethics: all actions must comply with the law and require appropriate authorization.

WITHOUT DIRECT ACCESS TO THE TARGET DEVICE

THESE METHODS RELY ON REMOTE INTERACTION WITH THE TARGET OR THE EXPLOITATION OF VARIOUS DIGITAL SERVICES.

SOCIAL ENGINEERING

The most underestimated, yet often extremely effective method.



POSSIBLE PRETEXTS

- Bank employee "Security department"
- Delivery service "Confirming the address"
- Technical support "Resolving a problem"
- Government agency "Official request"

Hacking the person, not the device.

Psychology, trust and plausibility.

REMOTE INTERACTION WITHOUT PHYSICAL ACCESS



TRUST AND PERSUASION

OPEN-SOURCE ANALYSIS

Analyzing social media geotags and public maps.
Public profiles reveal more than they seem to.

DATA SOURCES

- Social media
- Posts and photos
- Geotags and check-ins
- Reviews and comments
- Public maps
- Profiles and resumes





DIGITAL PROFILE

INTERESTS
HABITS
SCHEDULE
SOCIAL CONNECTIONS
LOCATION

CLOSE ANALYSIS OF PUBLIC PROFILES AND MENTIONS OFTEN REVEALS NOT ONLY THE CITY, BUT ALSO FAVORITE CAFES, ROUTES AND WORKPLACE.

1 OPEN DATA

Collecting information from available sources (social media, maps, forums, reviews, chats, etc.).

2 BEHAVIOR ANALYSIS

Identifying patterns, habits, interests, routes and connections of the target.

3 BUILDING A PRETEXT

Creating a convincing pretext for the target's context and choosing a communication channel.

4 CONTACT WITH THE TARGET

Making contact under a pretext and building trust to obtain the required information.

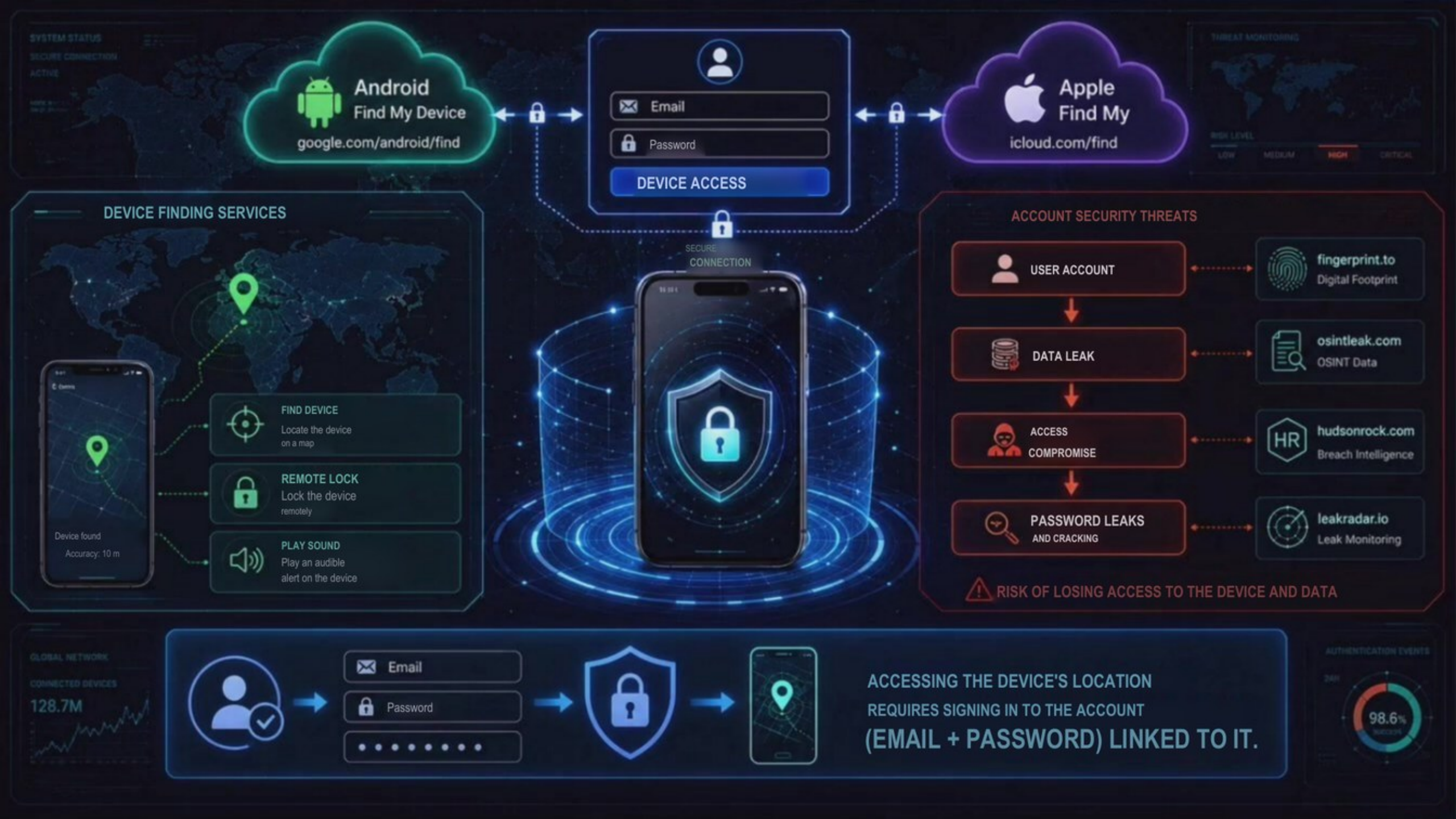
5 OBTAINING INFORMATION

Obtaining needed data: access, documents, location, etc.

All methods require a lawful basis and a thorough understanding of ethical standards.

Unauthorized surveillance is a criminal offense.


1. MESSAGE
2. FOLLOW THE LINK
3. REQUEST ACCESS TO GEOLOCATION
4. OBTAIN COORDINATES
5. TRANSMIT DATA
55.7558° N
37.6173° E
DELIVERY CHANNELS
DISGUISED LINK
ELECTRONIC MAIL
MESSENGER
SMS
SOCIAL NETWORK
https://bit.ly/xyz123
NEWS
DOCUMENT
EVENT INVITATION
DELIVERY NOTIFICATION
10:30
Friday, May 24
New message
Hi! These are photos from our event.
Take a look and find yourself!
https://bit.ly/xyz123
Tap to open the link
LOCATION FINDING
GPS SATELLITES
High accuracy
CELL TOWERS
Triangulation
WI-FI ACCESS POINTS
Local positioning
IP GEOLOCATION
By IP address
GEOLOGGERS (EXAMPLES)
github.com/thewhiteh4t/seeker
github.com/jofpin/trape
github.com/cryptomarauder/TrackUrl
github.com/Bafomet666/Bigbro
github.com/spyboy-productions/r4ven
iplogger.org/location-tracker/
DATA TRANSFER
HTML5 GEO API
GPS
high accuracy
WI-FI
urban navigation
LBS
mobile networks
IP
approximate location
HTML5 Geo API
USER'S BROWSER
PERMISSION REQUEST
Allow access to your location?
Allow
Block
55.7558° N
37.6173° E
COORDINATES
REMOTE WEB RESOURCE
DATA TRANSFER
USER DATA
Coordinates
Request time
IP address
Browser information
Device
ACTIVITY


Android
Find My Device
google.com/android/find
Email
Password
DEVICE ACCESS
Apple
Find My
icloud.com/find
DEVICE FINDING SERVICES
FIND DEVICE
Locate the device on a map
REMOTE LOCK
Lock the device remotely
PLAY SOUND
Play an audible alert on the device
Device found
Accuracy: 10 m
SECURE CONNECTION
ACCOUNT SECURITY THREATS
USER ACCOUNT
DATA LEAK
ACCESS COMPROMISE
PASSWORD LEAKS AND CRACKING
fingerprint.to
Digital Footprint
osintleak.com
OSINT Data
hudsonrock.com
Breach Intelligence
leakradar.io
Leak Monitoring
RISK OF LOSING ACCESS TO THE DEVICE AND DATA
Email
Password
ACCESSING THE DEVICE'S LOCATION
REQUIRES SIGNING IN TO THE ACCOUNT
(EMAIL + PASSWORD) LINKED TO IT.

YOUR SMARTPHONE CONSTANTLY TELLS THE WORLD WHERE IT IS

You do not need hacking skills to listen to that signal - a free app is enough.

WiGLE

A global database of access points and cell towers. People worldwide upload the results of Wi-Fi and Bluetooth scans.



nRF Connect

A professional tool for Bluetooth device developers, now a standard for monitoring BLE traffic.



LightBlue Explorer

An nRF Connect alternative for iOS and macOS. An easy interface, fast scanning and connections to BLE devices to inspect their characteristics.



BLE Radar

A specialized utility that displays devices in space in real time, estimating distance from signal strength.



YOUR SMARTPHONE: A TRANSMITTER OF IDENTIFIERS



HOW IT WORKS



1. SMARTPHONES TRANSMIT BLE SIGNALS
2. THE APP SCANS THE SURROUNDINGS
3. IDENTIFIES DEVICES AND DISTANCES
4. SHOWS THEM ON A MAP IN REAL TIME

REAL-TIME MAP OF DETECTED DEVICES



WHAT YOU SEE AFTER 30 SECONDS

- EXACT DEVICE MODELS (iPhone 15 Pro, Samsung Galaxy S23, AirPods Pro, etc.)
- DISTANCE TO THEM WITH SURPRISING ACCURACY
- THEIR COORDINATES ON A MAP

OBSERVATION EXAMPLE



IN REAL TIME, YOU WATCH **THE MOVEMENT OF THE DIGITAL "GHOSTS"** OF YOUR NEIGHBORS, COLLEAGUES AND PASSERS-BY.



PRIVACY RISKS



- PASSIVE MOVEMENT **TRACKING**
- PROFILING **AND BEHAVIORAL** ANALYSIS
- DEANONYMIZING **DEVICES AND USERS**
- LEAKS OF DATA ON PRESENCE AND ACTIVITY

EVOLUTION OF LOCATION FINDING



SOURCES OF LOCATION DATA



BLUETOOTH TRACKERS VS. AN "INNOCENT" EARBUD

ONE SMALL DEVICE, TWO SCENARIOS. HOW EASY IT IS TO GO UNNOTICED.

BLUETOOTH TRACKERS: CONVENIENCE AND RISKS



AirTag



Tile

TRACKER VULNERABILITIES

- iOS and Android warn when they detect unknown trackers
- Many apps scan the airwaves for tracker signals
- A tracker can be spotted during a careful visual inspection

EXAMPLES OF DETECTION APPS

- Tracker Detect (Android & iOS)
- DontTrack (Android)
- AirGuard (iOS)
- BLE Scanner (Android)

TWO DEVICES. TWO PERCEPTIONS.



VS

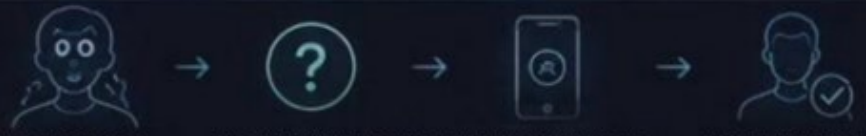
SUSPICIOUS	ORDINARY
Tracker = surveillance device	Earbud = lost property
Raises suspicion	Does not raise suspicion
High risk of detection	Low risk of detection

POSSIBLE PLACES TO "ACCIDENTALLY LOSE" AN EARBUD



BAG | UNDER A CAR SEAT | JACKET POCKET | OFFICE / HOME | LOCKER ROOM / GYM

HOW PEOPLE REACT TO FINDING AN EARBUD



OH, SOMEONE LOST AN EARBUD! → THROW IT AWAY? IT MIGHT COME IN HANDY. → I'LL TRY CONNECTING IT (NOT ALWAYS SUCCESSFUL) → LEAVE IT IN PLAIN SIGHT OR KEEP IT

HOW EARBUD TRACKING WORKS IN THE APPLE ECOSYSTEM

1. THE EARBUD IS LINKED TO THE ATTACKER'S APPLE ID
2. THE DEVICE TRANSMITS A SIGNAL VIA BLUETOOTH
3. NEARBY DEVICES FROM APPLE PICK UP THE SIGNAL
4. DATA IS ENCRYPTED AND SENT TO ICLOUD
5. THE LOCATION APPEARS IN THE FIND MY APP



ADVANTAGES OF AN EARBUD AS A TRACKER

- Small and unobtrusive
- An ordinary accessory that does not raise suspicion
- Difficult for scanners to detect
- Part of the Apple ecosystem (precise tracking)

MOVEMENT MAP (EXAMPLE)



IMPORTANT TO REMEMBER Using others' devices for covert tracking may violate the law and human rights.
This material is for information only, to raise awareness of the risks.

ADINT (Advertising Intelligence)

SOURCES OF ADVERTISING DATA

1 SEARCH PLATFORMS
AUDIENCES
AD SEGMENTS
ANALYTICS
ENGAGEMENT STATISTICS
ANONYMIZED DATA
72%

2 SOCIAL NETWORKS
AUDIENCES
AD SEGMENTS
ANALYTICS
ENGAGEMENT STATISTICS
ANONYMIZED DATA
65%

3 TELECOM OPERATORS
AUDIENCES
AD SEGMENTS
ANALYTICS
ENGAGEMENT STATISTICS
ANONYMIZED DATA
58%

UNIFIED ADVERTISING ECOSYSTEM



GEOGRAPHIC ANALYTICS



GEOFENCES
ZONE A
ZONE B
ZONE C
ZONE D

DEVICES
12 589
ACTIVE DEVICES

SIGNALS
24 786
EVENTS

TIMESTAMPS
10:15 ACTIVITY
10:27 AD VIEW
10:42 AD CLICK
11:03 LOCATION VISIT

ANALYTICAL MARKERS
POINTS OF INTEREST
MOVEMENT PATHS
VISIT FREQUENCY
AD INTERACTIONS

ACTIVITY OVER TIME

ZONE VISITS

DEVICE TYPES
48% 32% 15% 5%

1. IDENTIFIERS
IDFA

2. ADVERTISING PLATFORMS

3. AUDIENCE SEGMENTS
INTERESTS
DEMOGRAPHICS
BEHAVIOR
PURCHASES

4. GEOANALYTICS
GEOFENCES
ROUTES
VISITS
FREQUENCY

5. BEHAVIOR MODELS
PREFERENCES
ACTIVITY
HABITS
REACTIONS

6. DIGITAL PROFILE

CAPABILITIES OF ADVERTISING DATA

SOCIAL PROFILING
OF A USER
OR GROUP OF PEOPLE

MOVEMENT TRACKING
OR MONITORING

IDENTIFYING SOCIAL
CONNECTIONS AND CONTACTS

COLLECTING USER DATA
IN A SPECIFIED AREA

GUIDANCE OF PRECISION
WEAPONS

DELIVERY AND
INSTALLATION OF SPYWARE

LIVE DATA STREAM
REQUESTS / SEC
1.28M
ACTIVE DEVICES
8.74M
EVENTS TODAY
2.59B


Speed Dial
Search or enter a web address
PERSONAL
TELEGRAM
WEB RESOURCES
CRYPTOCURRENCIES
CONTACTS
RESEARCH
SECURITY CHECKS
WORKSPACE
Oslo
Choose your city
20 °C
PHONE
EMAIL
HLR, PING, REGISTRATION
REGISTRATION SEARCH
LEAKS
BILLING AND CALL RECORDS
GEOLOCATION
BASE STATIONS
IMEI
FIND DEVICE
GEOLOGGING
ADINT
IPLOGGER [HTML5 GEO]
R4VEN [HTML5 GEO]
BIGBRO [HTML5 GEO]
TRACKURL [HTML5 GEO]
TRAPE [HTML5 GEO]
SEEKER [HTML5 GEO]
NGROK [HTML5 GEO]
People
Locations
Events
Connections
OSINTbro
FIND THE TRUTH. CONNECT THE DOTS.
Case #2701
Digital Footprint
- WHO
- WHAT
- WHERE
- WHEN
- WHY
- HOW
MATCH FOUND
DOWNLOAD

CONTACT CARD

