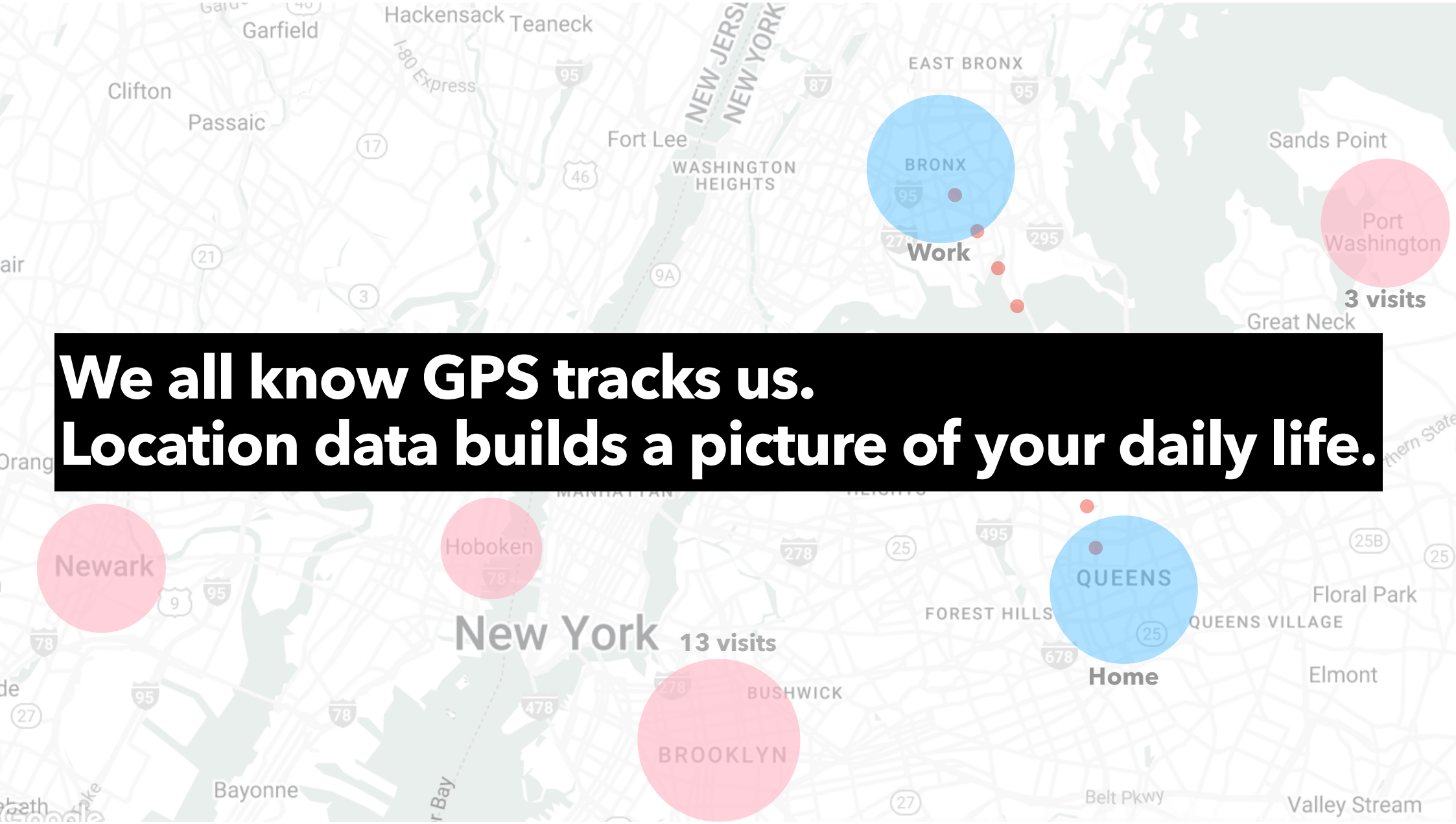
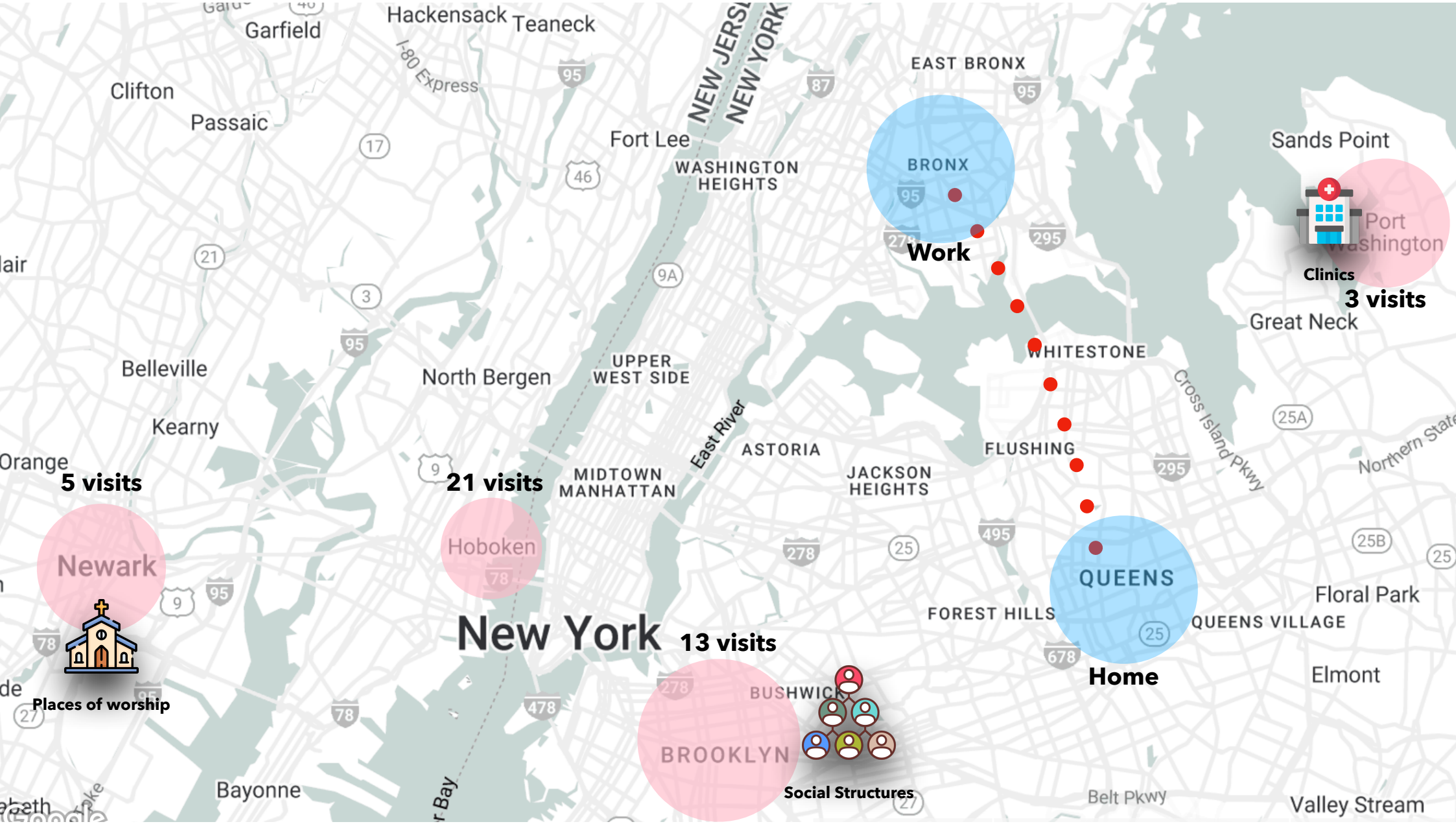
Your Signal, Their Data: An Empirical Privacy Analysis of Wireless-scanning SDKs in Android

Aniketh Girish

Joel Reardon, Juan Tapiador, Srdjan Matic, Narseo Vallina-Rodriguez

21 October 2025
REDIMadrid 2025
Madrid, Spain


Garfield
Hackensack
Teaneck
Clifton
Passaic
I-80 Express
NEW JERSEY
NEW YORK
EAST BRONX
Fort Lee
WASHINGTON HEIGHTS
BRONX
Work
Sands Point
Port Washington
3 visits
Great Neck
We all know GPS tracks us.
Location data builds a picture of your daily life.
Newark
Hoboken
New York
13 visits
QUEENS
FOREST HILLS
QUEENS VILLAGE
Floral Park
Home
Elmont
BUSHWICK
BROOKLYN
Bayonne
Belt Pkwy
Valley Stream


Garfield
Hackensack
Teaneck
Clifton
Passaic
I-80 Express
Fort Lee
NEW JERSEY
NEW YORK
WASHINGTON HEIGHTS
EAST BRONX
BRONX
Work
Sands Point
Port Washington
Clinics
3 visits
Great Neck
WHITESTONE
Belleville
North Bergen
UPPER WEST SIDE
Kearny
East River
ASTORIA
FLUSHING
Cross Island Pkwy
Northern State
Orange
5 visits
21 visits
MIDTOWN MANHATTAN
JACKSON HEIGHTS
Newark
Hoboken
QUEENS
Floral Park
FOREST HILLS
QUEENS VILLAGE
New York
13 visits
Home
Elmont
BUSHWICK
BROOKLYN
Places of worship
Social Structures
Bayonne
Belt Pkwy
Valley Stream

Please Forget Where I Was Last Summer:

BY DHRUV MEHROTRA AND DELL CAMERON SECURITY MAR 28, 2024 7:00 AM

Jeffrey Epstein's Island Visitors Exposed by Data Broker

A WIRED investigation uncovered coordinates collected by a controversial data broker that reveal sensitive information about visitors to an island once owned by Epstein, the notorious sex offender.

Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen & Vincent D. Blondel

PIXELS • INVESTIGATIONS

Personal data for sale: The out-of-control industry of data brokers

By Adrien Sénécat, Martin Untersinger, Elsa Delmas, Léa Girardot and Anne Morel

Published on February 12, 2025, at 8:00 pm (Paris), updated on February 13, 2025, at 9:42 am

7 min read Lire en français

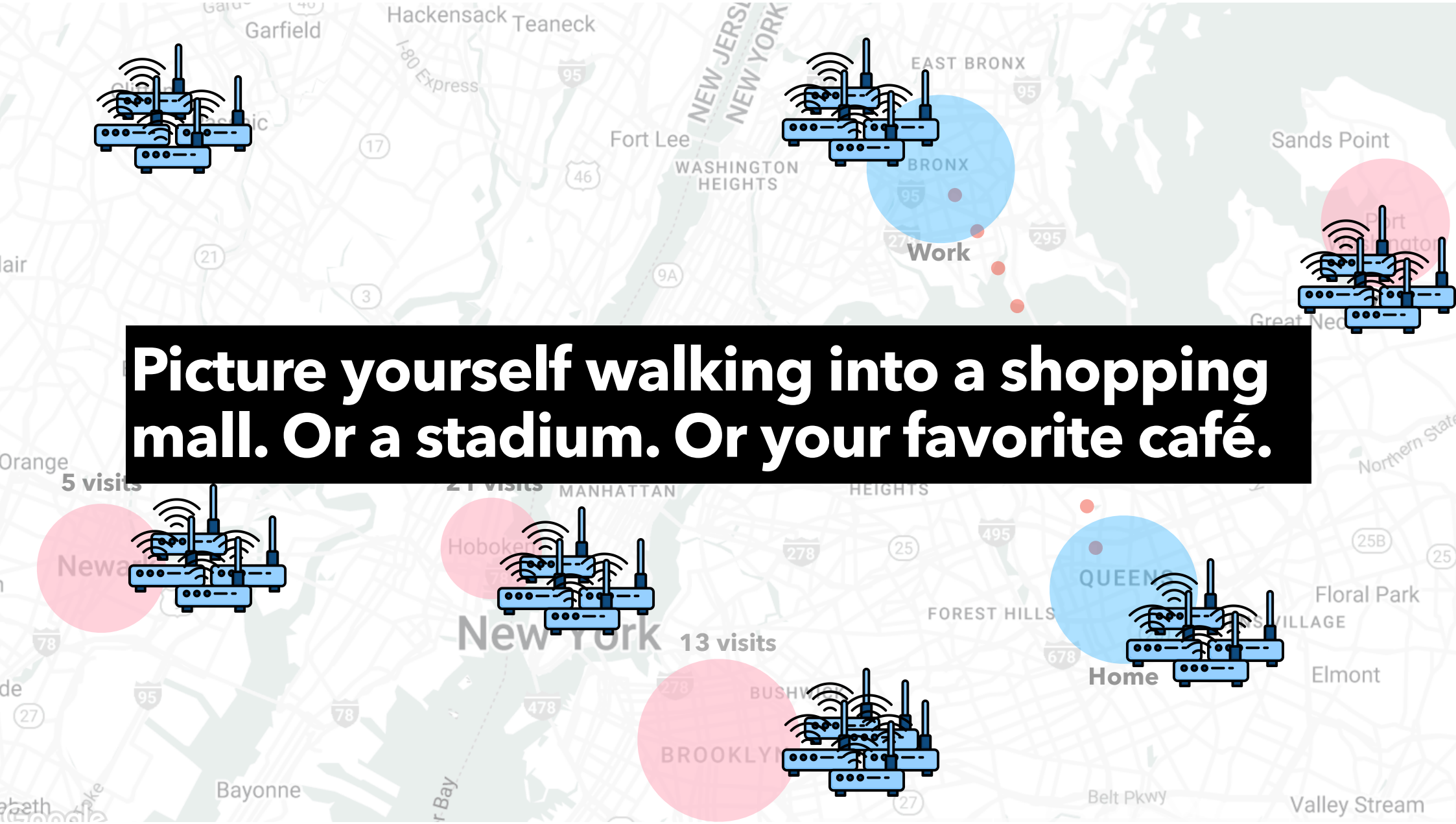
EXCLUSIVE POLITICS

House Investigating Company Selling Phone Location Data to Government Agencies

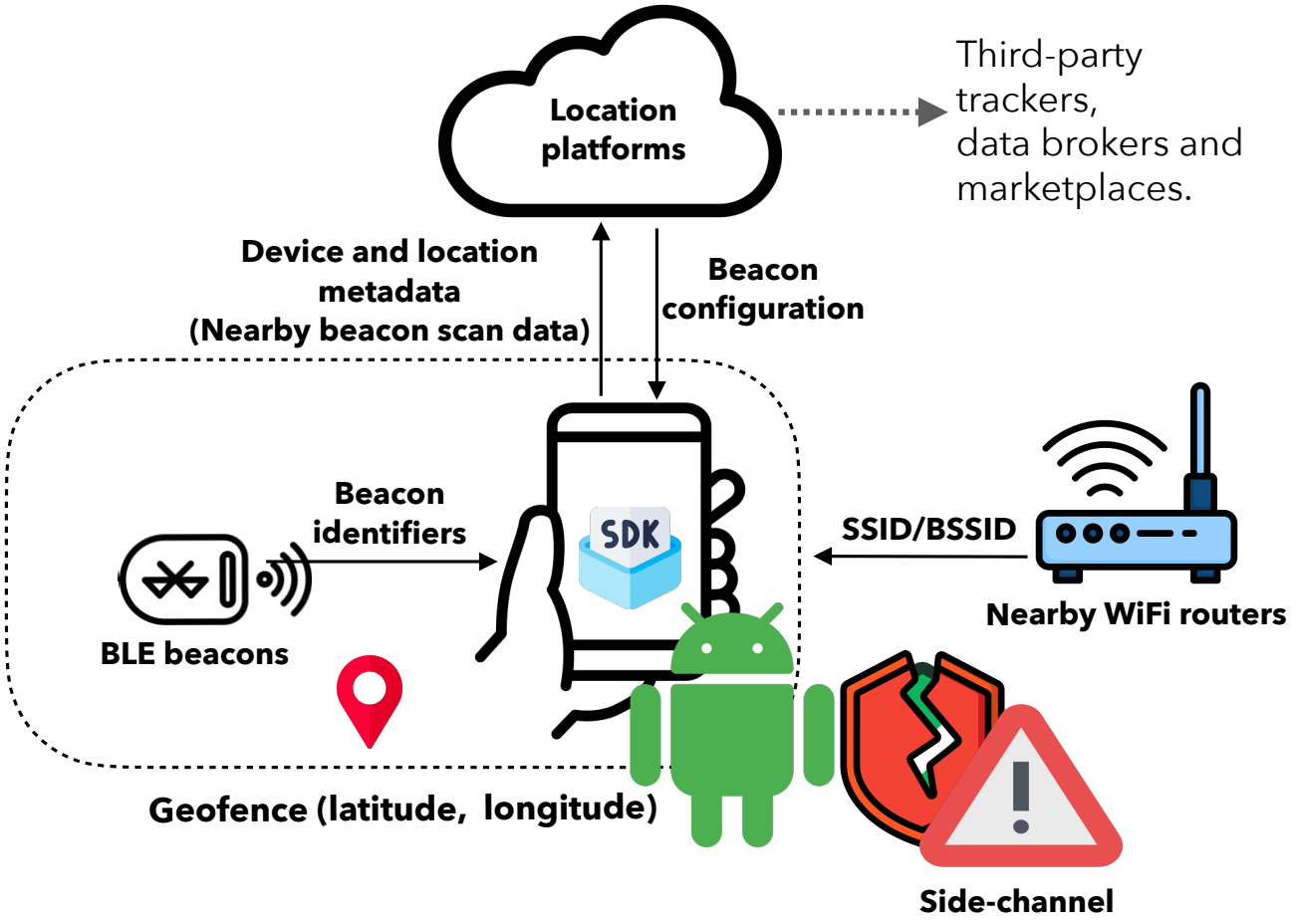
A Democratic-led committee said it was conducting an investigation of the products sold by data broker Venntel

By Byron Tau Follow

June 24, 2020 3:19 pm ET


Garfield
Hackensack
Teaneck
I-80 Express
NEW JERSEY
NEW YORK
EAST BRONX
Fort Lee
WASHINGTON HEIGHTS
BRONX
Work
Sands Point
Great Neck
Picture yourself walking into a shopping mall. Or a stadium. Or your favorite café.
Orange
5 visits
MANHATTAN
HEIGHTS
Hoboken
New York
13 visits
QUEENS
FOREST HILLS
Floral Park
Home
Elmont
BROOKLYN
Bayonne
Belt Pkwy
Valley Stream

How do they manifest?

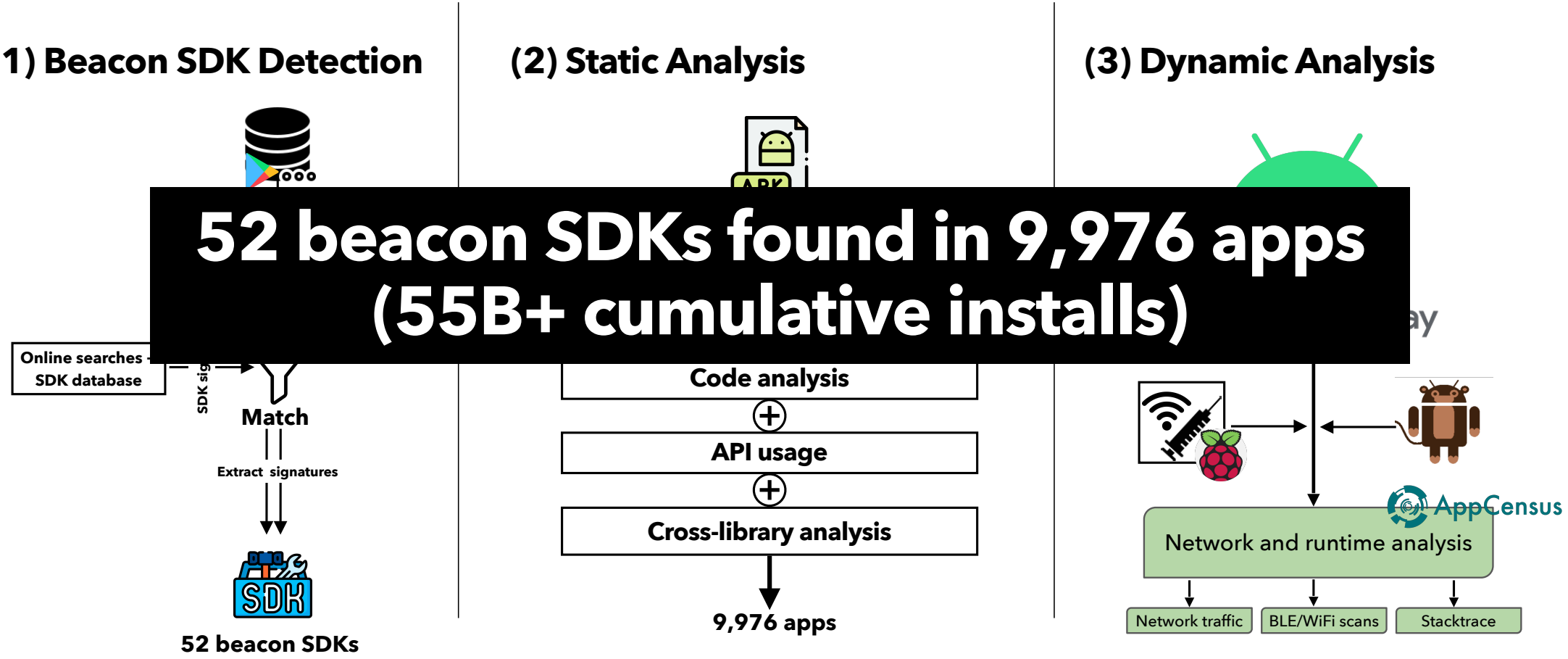


Linking geolocation data with user or device IDs like the Android Advertising ID (AAID) and MAC addresses make reversing users' identity and movement patterns straightforward!

Objectives: Characterize wireless SDKs

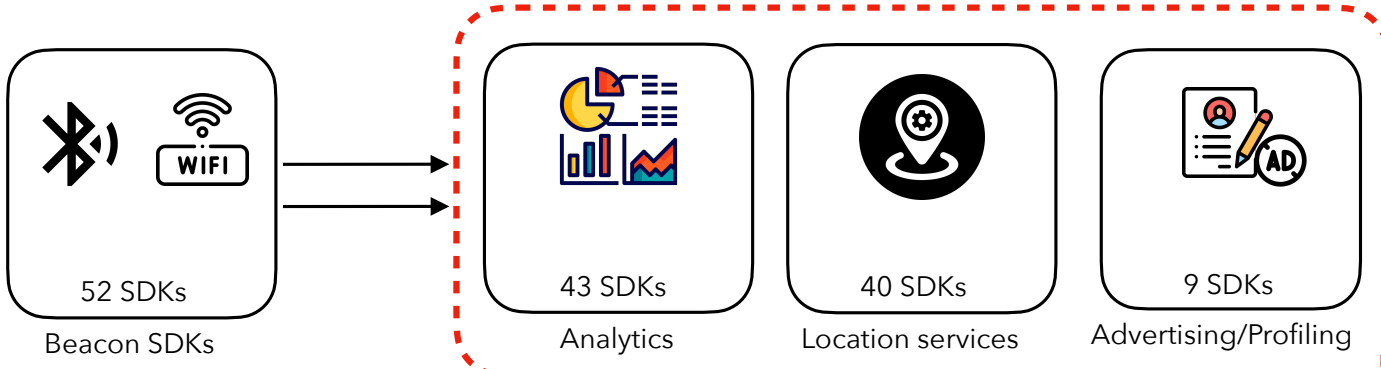
1. **Who** are the SDKs involved, and **what** data do they collect?
2. **How** do they share/synchronize IDs to map geolocation data with user identities?
3. **What** privacy risks arise?

Methodology



SDK & App Prevalence

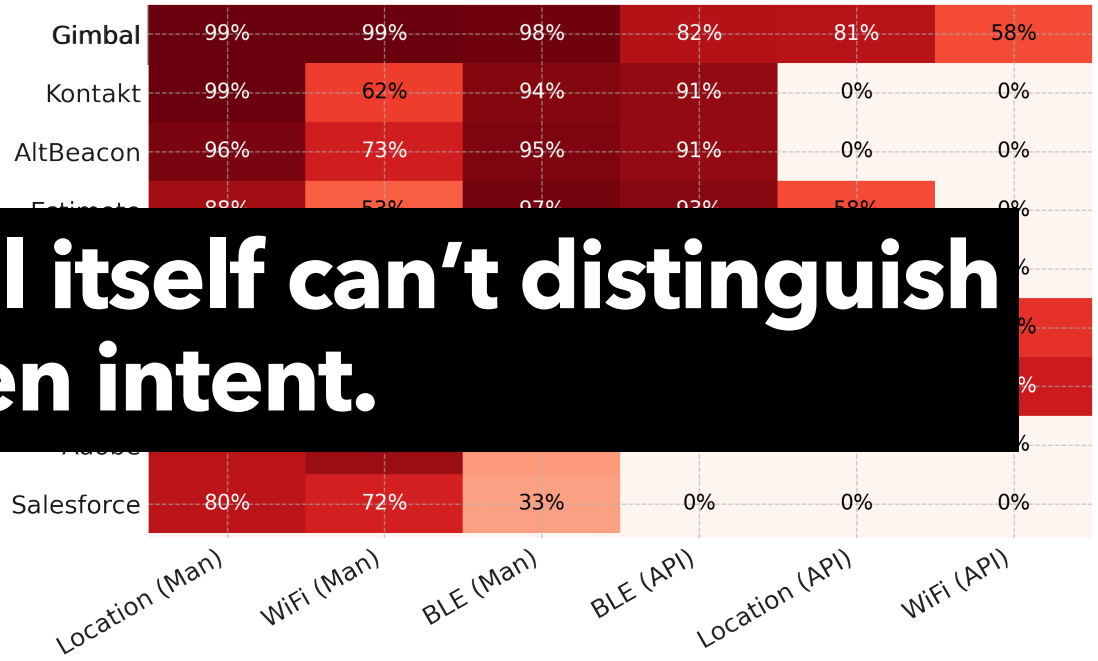
→ Beacon SDKs serve dual purpose



SDK	# Apps	Total Installs	Beacon Type			Purpose Type		
				WIFI	Integration	Analytics	Location	Advertising
ALT BEACON	4,022	5B	✓			✓	✓	
Adobe Experience Cloud	1,328	8B			✓	✓		✓
KOCHAVA	1,117	15B		✓	✓	✓	✓	✓
salesforce marketing cloud	1,080	6B			✓	✓	✓	
estimote	510	201M	✓			✓	✓	

Permission Analysis

- Most beacon-enabled apps request location, Wi-Fi, and BLE permissions – often more than they need.
- Some SDKs even use wireless APIs without declaring the
- And
  func
- Marketing and analytics SDKs request similar permissions as beacon SDKs.
- Several SDKs appear over-permissioned – declaring more access than necessary.



The permission model itself can't distinguish between intent.

Privacy Analysis

- Bluetooth and Wi-Fi signals turned into a **covert location tracking infrastructure.**
- Users are not aware.
- **86%** of apps collect at least one sensitive data type (e.g., AAID, GPS, or wireless scan results)

KOCHAVA cuebiq

Yandex

Radar SDK

```
com.geomobile.tiendeo outbound to api.radar.io:443
POST /v1/logs HTTP/1.1
Content-Type: application/json
Host: api.radar.io
..
"androidid":"XXXXXXXXXXXXXX"
{
    "createdAt": 1720523270332,
    "level": "DEBUG",
    "message": "Ranged beacon | beacon.type = IBEACON; beacon.uuid = 01022022-
          fa0f-0100-00ac-dd1c6502da1c; beacon.major = 53479; beacon.minor =
          42571; beacon.rssi = -12"
},
{
    "createdAt": 1720523270334,
    "level": "DEBUG",
    "message": "Handling beacon entry | beacon.type = IBEACON; beacon.uuid =
          01022022-fa0f-0100-00ac-dd1c6502da1c; beacon.major = 53479; beacon.
          minor = 42571; beacon.rssi = -12"
},

"events":[], "nearbyGeofences":[{"_id":"6318a0381c18820019e1e07e", "live":true,
"type":"circle", "tag":"es.s.m","externalId": "103769","geometryCenter":
{"coordinates":[longtitude: -X.XXXXX,latitude: XX.XXX],"type":"Point"},
```

Exploitation of Outdated APIs for Location Inference

Exploits CVE-2020-0454 to access SSIDs.

→ **No need for location permissions.**

```
public void onCapabilitiesChanged(Network network, NetworkCapabilities networkCapabilities) {
    super.onCapabilitiesChanged(network, networkCapabilities);
    try {
     Matcher matcher = Pattern.compile("SSID: \"(.*)\"").matcher(networkCapabilities.toString());
       if (matcher.find()) {
            String group = matcher.group(1);
            if (!TextUtils.isEmpty(group)) {
                AndroidPieNetworkManager.this.hackedSsid = group;
            }
        }
    } catch (Exception e) {
        String str = AndroidPieNetworkManager.this.LOG_TAG;
        Logger.m88e(str, "Caught Exception reading SSID: " + e.getMessage());}}
```

→ **Deliberate attempt!**

Exploitation of Outdated APIs for Location Inference

Collect SSIDs, IMEI, DHCP/DNS data on ≤ Android 9.

→ **~9% of phones run Android 9.**

Network configs

WiFi scan results

```
com.douglas.main outbound to m.api.forter.com:443

POST /v1/data HTTP/1.1
Content-Type: application/json; charset=utf-8
Host: m.api.forter.com

  {"accountID": "",
  "data": {
    "currentNetworkType": "WiFi",
    "wifi": {
     "dhcp": {
       "dhcpAddr": "172.16.8.1",
       "dns1": "208.67.XXX.XXX",
       "gw": "172.16.X.X",
       "ipAddr": "172.16.X.XX",
       "leaseDur": "86400",
       "nm": "0.0.0.0"
     },
      "ipAddr": "172.16.X.XX",
     "scanResults": [
       {"caps": ["RSN-SAE-CCMP"],"ssid": "ABC-WIFII"},
       {"caps": ["RSN-SAE-CCMP"],"ssid": "XYZ-WIFII"}
     ]
```

Privacy Analysis

SDK (# of Apps)	# App. Installs	Glob. Pers.						App. Pers.	Glob. Rst.		App Rst.	WiFi/BLE scan						GPS	
		Boot ID	GSF ID	IMEI	HW ID	WiFi MAC	Email	Android ID	AAID	BLE Name	FID	BLE ibeacon MAC	ibeacon UUID	Router MAC	Router scan MAC	Router Scan SSID	Router SSID	Coarse gelog.	Fine geoloc.
Kochava (220)	2B							◇	★	★				★			★		
Yandex (220)	572M			◇		★		◇	★					★	★	★	★		
Amplitude (190)	988M			◇			◇	◇	★	★								★	★
Datadog (140)	146M			◇				◇	★		★			★			★	★	★
Sentry (81)	53M					◇		◇	★	◇	▾			★			★	★	★
Omniture (49)	1B					◇		◇	★								★	★	★
Forter (34)	297M			◇	◇			◇		◇						★	★		
Radar (33)	280M							◇	◇				★					★	★
Huq Sourcekit (24)	25M							◇	★	★	★			◇			◇	★	★
cellrebel (18)	134M													★			★	★	★
Vizbee (16)	164M							◇	★					★			★	★	★
Cuebiq (6)	50M								★					★	★	★	★	◇	◇
taobao (6)	1B			◇				◇						★					
My Tracker SDK (6)	132M								★					★			★		
AdsWizz (6)	9M								★								◇	★	★
phunware (5)	78K								★		★			◇			★	★	★
conviva (5)	134M							◇	★					★			★	★	★
PayPal (5)	100M		★	◇	◇			◇						★	◇		★	★	★
Singlespot (5)	30M								★			★							
Incognia (5)	38M	★						◇	★					★	★	★	★	★	★
Colocator (4)	395K							◇						★					
Swrve (3)	9M							◇	★										
JPush (3)	346K															★	★		
Kontakt (3)	23K											★							
Proxy Cloud (2)	7M													★	★	★	★	★	★
pingID (1)	3M					◇		◇								▾	★		
appICE (1)	3M								★					★			★	◇	◇
Tangerine (1)	3M								★								★		
Proximi.io (1)	162K												▾						

Identifier Linking: SDKs like **Kochava** and **Yandex** tie Wi-Fi or BLE scan data with device IDs (AAID, Android ID).

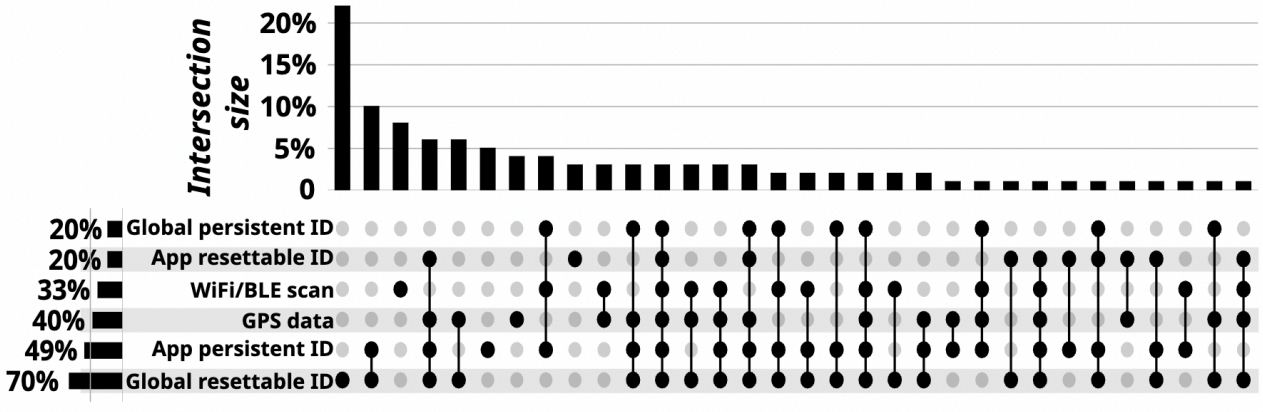
Cross-Source Fusion: Platforms such as **Radar** combine beacon data with **GPS** and **network metadata**.

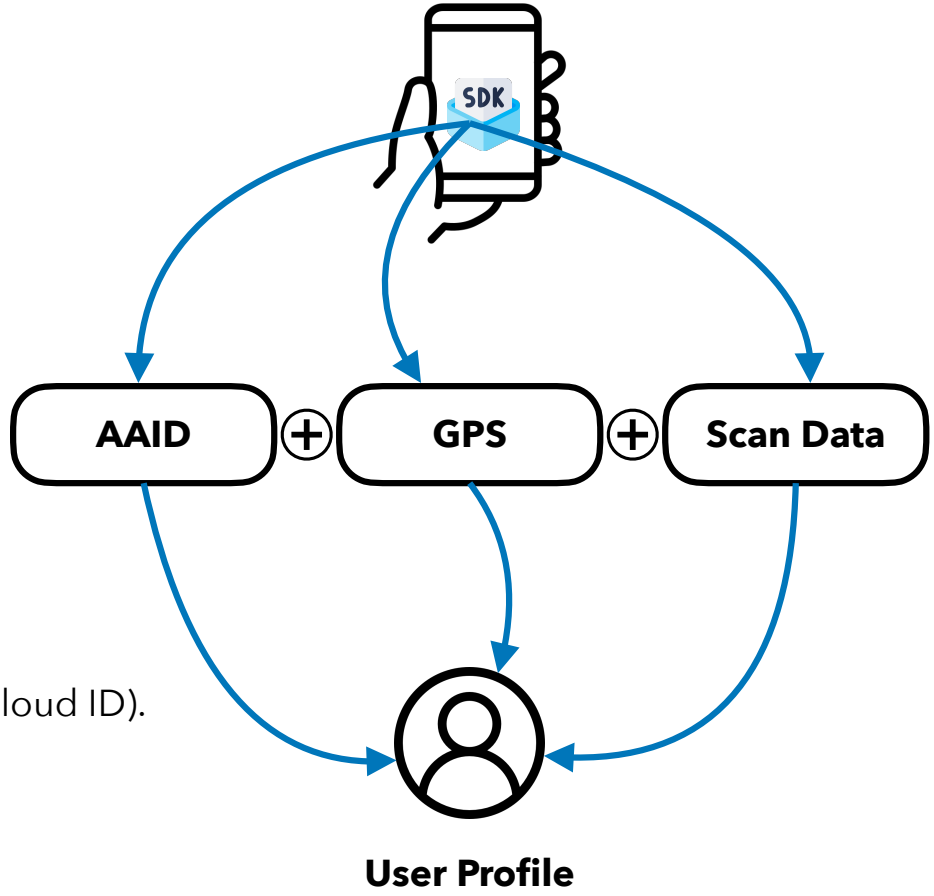
Tracking Resilience: Even after resets, these SDKs can re-identify users through overlapping signals.

Identifier Bridging

→ SDKs link resettable and persistent IDs.

→ Enables long-term profiling across apps and re-identification even after resets!





❌ 32% of SDKs perform ID bridging.

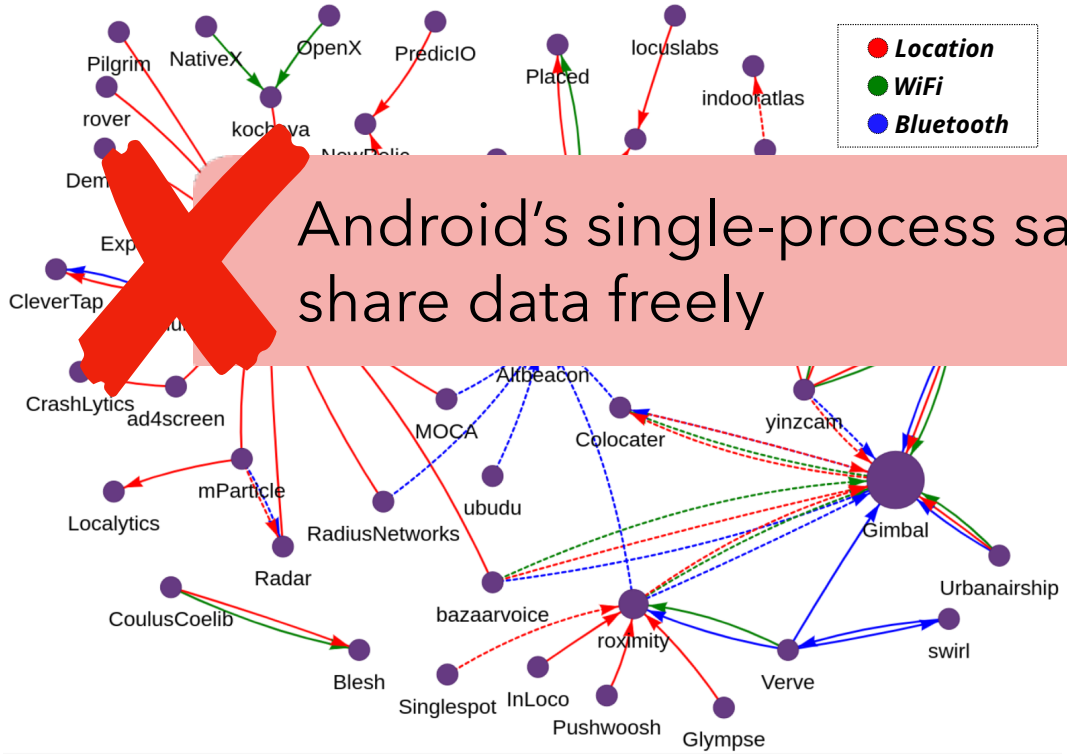
❌ Bridging with persistent proprietary identifiers (e.g., Adobe Marketing Cloud ID).

❌ Unvetted cross-library data sharing (e.g., Adobe ↔ Appsflyer).

SDK-to-SDK Sharing

➔ 28 SDKs exhibit extensive cross-library interactions.

➔ SDKs collude among themselves to share location data for tracking and advertising purposes.



Android's single-process sandbox model lets colluding SDKs to share data freely

(ii) Beacon SDK ↔ ATS SDK

24 beacon SDKs feed wireless scan & geolocation data to 21 non-beacon advertising/analytics SDKs.

Potential Non-Compliance with Platform Policies

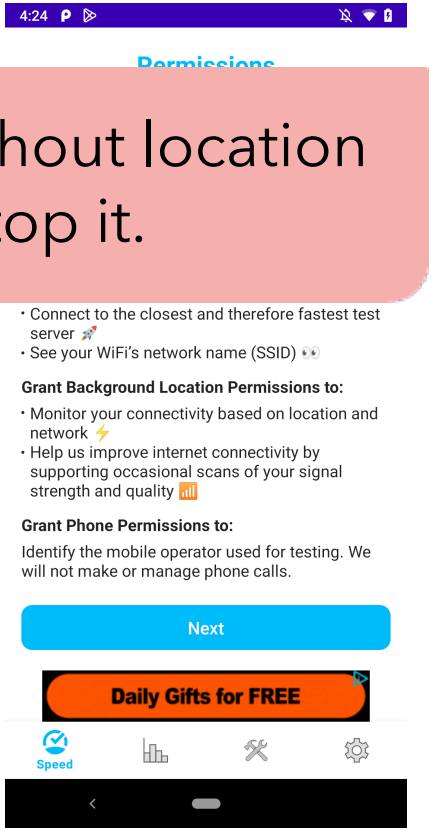
- ❌ Collecting location data for ads or linking IDs may violate Play Store policies.
- ❌ 71% of apps provide no rationale for requesting location permissions.
- ❌ O

Users are being tracked via wireless signals—even without location permissions. Platform safeguards are insufficient to stop it.

Use of Location Data for Ads

Apps that extend usage of permission based device location data for serving ads are subject to the Personal and Sensitive Information policy, and must also comply with the following requirements:

- Use or collection of permission based device location data for advertising purposes must be clear to the user and documented in the app's mandatory privacy policy, including linking to any relevant ad network privacy policies addressing location data use.
- In accordance with Location Permissions requirements, location permissions may only be requested to implement current features or services within your app, and may not request device location permissions solely for the use of ads.



What Needs to Change?

Platform & Regulatory Accountability

- Proactive runtime audits of SDK behavior
- SDK sandboxing and tighter permission boundaries
- Stronger enforcement against ID bridging
- Mandatory public disclosure of SDK data practices
- Transparent, verifiable user consent flows

Defense Measures

- Disable Wi-Fi and Bluetooth Scanning
- Set Bluetooth to Hidden Mode
- Restrict App Permissions Aggressively

Conclusion

First Large-Scale Characterization

- First hybrid static + dynamic analysis of wireless-scanning SDKs.
- 52 commercial beacon SDKs across 9,976 apps (55 B+ installs).
- Identified cross-SDK interactions where SDKs exchange data within the same app.

Privacy Impact

- 86% of apps exfiltrate sensitive data (IDs, Wi-Fi/Bluetooth scans, GPS).
- 32% of SDKs link resettable and persistent IDs → persistent fingerprints.

Transparency Failures

- 71% of apps give no rationale for location/Bluetooth permissions.
- Only 5 out of 52 SDKs explain their data collection via permission rationale.
- Indicates systemic lack of user transparency about why sensitive permissions are requested.

Disclosure

- Findings reported to Google and EU regulators (AEPD, CNIL, EDPS).
- Remediation discussions ongoing with platform and policy stakeholders.

Thank you!

Aniketh Girish
aniketh.girish@networks.imdea.org

SCAN ME

Datasets and code

Backup

Key takeaways

→ **Android apps can access Wi-Fi and Bluetooth scan data through embedded SDKs.**
These signals act as precise location proxies, even when GPS is disabled.

→ **SDKs often collect this scan data alongside device identifiers.**
By linking resettable IDs (like the AAID) with persistent ones (e.g., Android ID, MACs), they perform *ID bridging*—reconstructing long-term user profiles.

→ **This defeats modern privacy protections like Advertising ID resets.**
Enabling persistent cross-app tracking without user awareness or consent.

Conclusion

- **First large-scale characterization:** First hybrid static + dynamic analysis of 52 commercial beacon SDKs across 9,976 Android apps (55B+ installs), revealing hidden data flows and cross-SDK interactions.
- **Privacy Impact:** 86 % of apps exfiltrate PII (device IDs, Wi-Fi/BLE scans, GPS), with 32 % of SDKs bridging resettable and persistent IDs alongside sensor data—creating persistent user fingerprints.
- **Transparency Failures**: 71 % of apps offer no location-permission and only five SDKs even attempt to explain permissions, highlighting systemic over-asking and under-disclosure.
- **Disclosure:** We disclosed to responsible parties, ongoing efforts for remediation.

Thank you!

Aniketh Girish
aniketh.girish@networks.imdea.org

SCAN ME

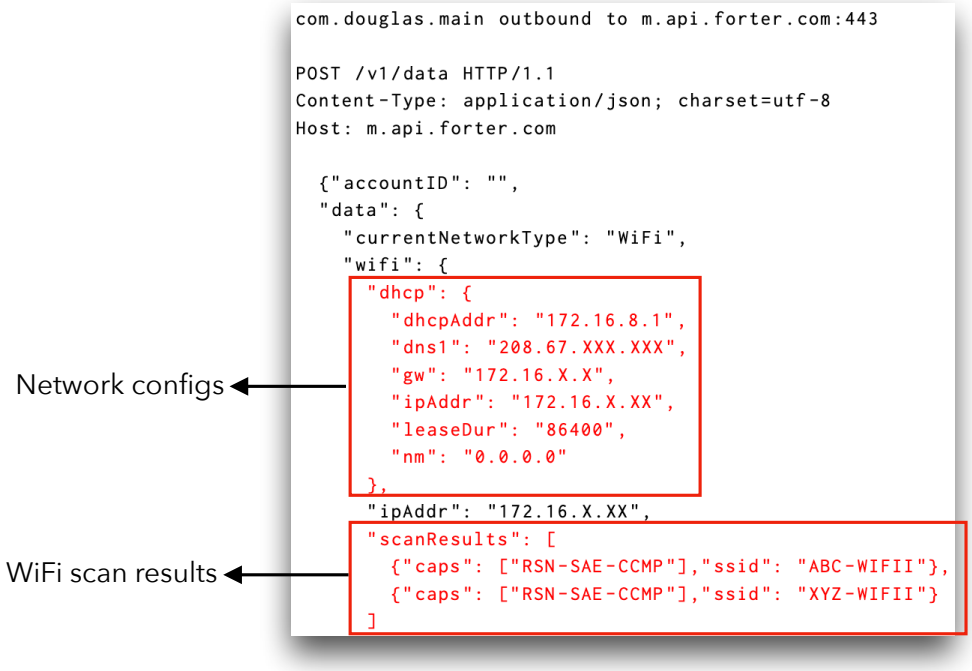
Datasets and code available here: https://github.com/wireless-scanning-SDKs/wireless-beacon-analysis

Exploitation of Outdated APIs for Location Inference

FORTER®

Collect SSIDs, IMEI, DHCP/DNS data on ≤ Android 9.

→ ~9% of phones run Android 9.



What Needs to Change?

Platform Policy Enforcement

- Proactive Runtime Audits by Platforms
- SDK Sandboxing and Isolation
- Stricter Enforcement Against ID Bridging

Regulation and Transparency

- Stronger Regulatory Oversight on SDK Practices
- Mandatory Disclosure of SDK Data Practices
- Transparent and Verifiable Consent Mechanisms

Defense Measures

- Disable Wi-Fi and Bluetooth Scanning
- Set Bluetooth to Hidden Mode
- Restrict App Permissions Aggressively

Conclusion

First Large-Scale Characterization

- First hybrid static + dynamic analysis targeting wireless-scanning SDKs.
- Analyzed 52 commercial beacon SDKs embedded across 9,976 Android apps totaling 55 billion+ installs.
- Identified cross-SDK interactions where SDKs exchange data within the same app.

Privacy Impact

- 86% of apps exfiltrate sensitive data: device IDs, Wi-Fi/Bluetooth scan results, GPS locations.
- 32% of SDKs perform ID bridging: linking resettable (AAID) and persistent (Android ID, MAC addresses) identifiers.
- Creation of persistent user fingerprints that are difficult to reset or anonymize.

Transparency Failures

- 71% of apps fail to provide permission rationales when requesting location or Bluetooth access.
- Only 5 out of 52 SDKs explain their data collection via permission rationale.
- Indicates systemic lack of user transparency about why sensitive permissions are requested.

Disclosure

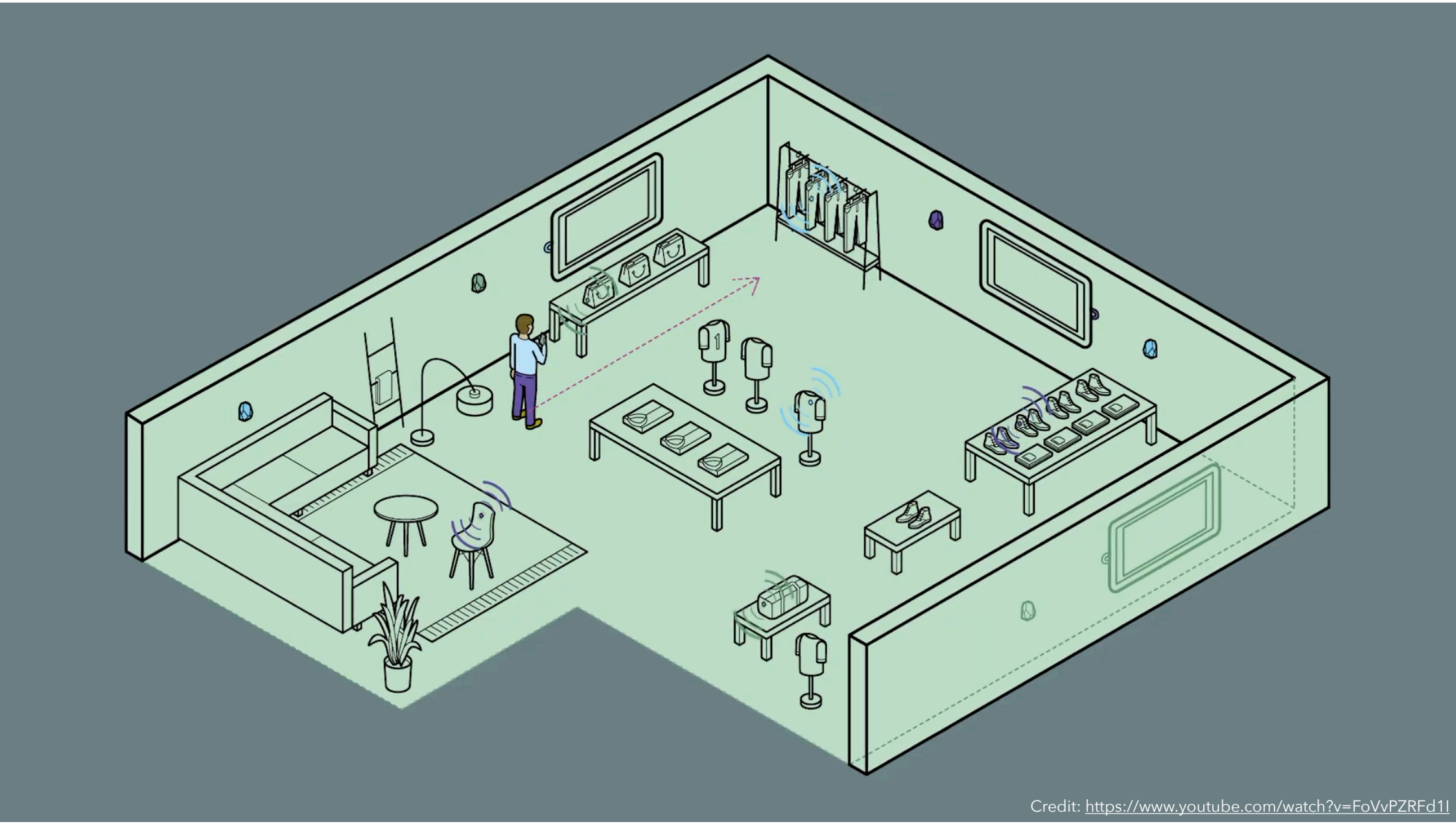
- Findings responsibly disclosed to Google and European privacy regulators (AEPD, CNIL, EDPS).
- Ongoing remediation discussions with platform and policy stakeholders.

Thank you!

Aniketh Girish
aniketh.girish@networks.imdea.org

SCAN ME

Datasets and code



Credit: https://www.youtube.com/watch?v=FoVvPZRFd1I