CUJO AI

MAC Address Randomization

Solving Device Identification with CUJO AI

2020

Table of Contents

What Is a MAC Address

A media access control (MAC) address is a hardware identifier used in networking. MAC addresses play a crucial role in OSI Layer 2 communications (the data link layer). Antenna chips in mobile devices use MAC addresses to discover and connect to local networks, including Wi-Fi routers.

How MAC Addresses Are Used for Device Identification

Every wireless networking device, including mobile phones and smart watches, probes network routers around it. These probe requests carry the device's MAC address, a unique set of 48 or 64 bits, much like a car's license plate. Once a device connects to and authenticates with a network, its MAC address can be added to a whitelist to avoid re-authentication every time the device is in the area. Using a MAC address as a unique identifier is a common, albeit discouraged, practice.

A MAC address can also present several key data points about a device by itself: its model and manufacturer, connection type (unicast, multicast, broadcast).

> **Many network operators, Wi-Fi hotspot providers, and public spaces use MAC addresses as unique device identifiers for authentication. This lets them track usage statistics, create network steering solutions, and country-wide instant access hotspot networks.**

Parallel to these legitimate uses for identification, marketing trackers also use MAC address information from Wi-Fi beacons and probe attacks to track client foot traffic and location data. A static MAC address can be reliably attributed to a particular person, according to researchers.[1]

[1] *https://hal.inria.fr/hal-00858324/document*

Reliance on MAC Addresses in Network Management

It is common to use MAC addresses to identify and authenticate devices. This is an unintended and discouraged practice in networking, as MAC addresses should only be used for L2 communication. Any other solutions hinged on this data point are bound to run into issues, as most mobile devices have the option to randomize their MAC addresses.

Parental controls use MAC address blacklists to prevent some devices from accessing harmful and mature content.

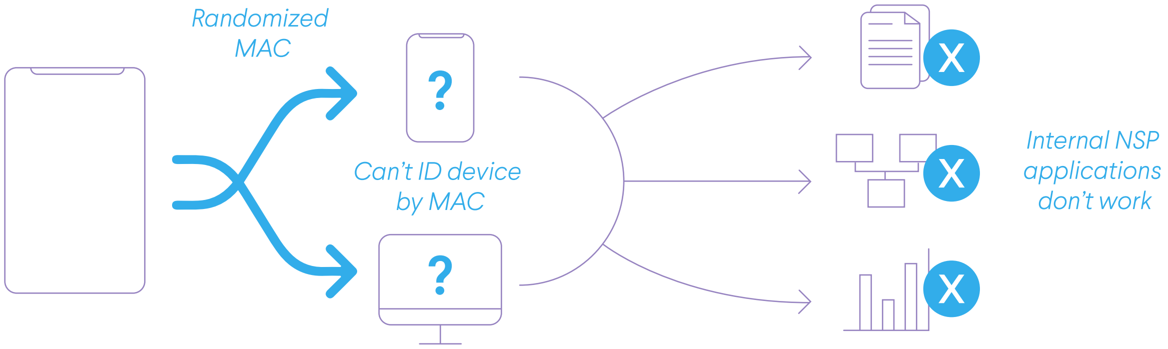
Network service providers use MAC addresses to estimate traffic consumption and gain statistical insights into their network usage.

Broadband analysts use MAC addresses to identify device types for traffic steering and network load management.

Users group and manage devices by their MAC addresses on their home networks.

Customer service desks use MAC addresses for basic device identification during troubleshooting.

Policy attribution and authentication is sometimes based on identifying devices by their MAC addresses.



Every use case above depends on MAC addresses being unique and static. If a device has a single address, it is easy to set up controls once and forget it. MAC randomization is quickly changing reality and making these solutions obsolete.

What Is MAC Address Randomization

MAC address randomization is the practice of generating a unique and unpredictable hardware address. In the past, changing one's MAC address with the help of software was called 'MAC address spoofing' and used only by a small minority of power-users. According to device intelligence analysts at CUJO AI, **close to 30% of all mobile devices are expected to adopt MAC randomization by early 2021.**

Why Is MAC Randomization on the Rise?

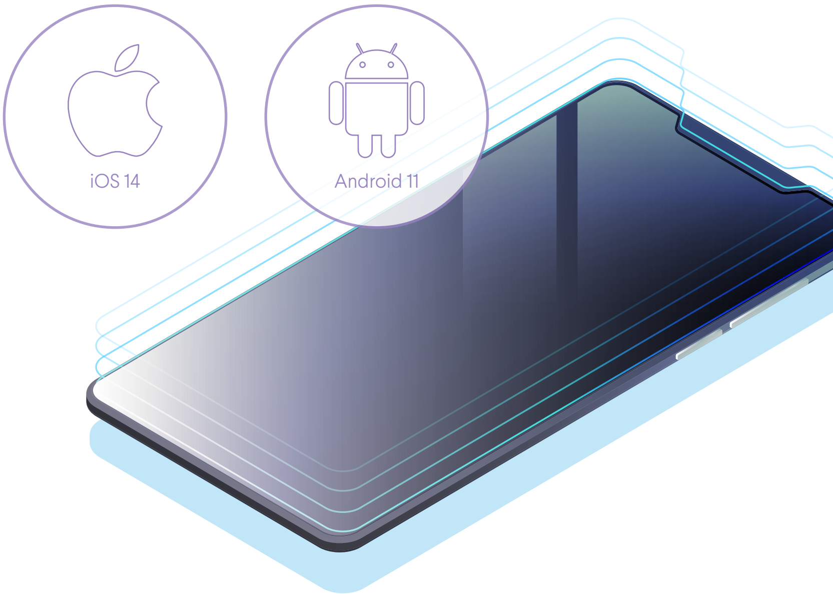
MAC randomization is a privacy practice that is becoming the default standard in mobile devices. Manufacturers want to protect users from probing surrounding networks with the same MAC address, as it makes their owners easy to track. MAC randomization was available on most devices for over 5 years, but now it is turned ON by default on iOS 14 and some Android 11 devices.

MAC ADDRESSES

00:1C:A2:01:A3:45
00:A0:C9:14:C8:29
00:1B:44:11:3A:B7
00:06:5B:BC:7A:C7

The Challenge From iOS 14, WatchOS 7 and Android 11

MAC randomization is ON by default in all iOS 14, WatchOS 7, and some Android 11 devices. It means that many network operators will face issues with device detection, Wi-Fi steering, customer service authentication, and even parental control solutions.



Today, relying on MAC addresses for device identification and authentication is no longer an option, as forcing users to turn MAC randomization OFF might impact their privacy. CUJO AI is here to help network service providers that want to use privacy-first solutions for large scale device statistics and model detection without relying on MAC addresses.

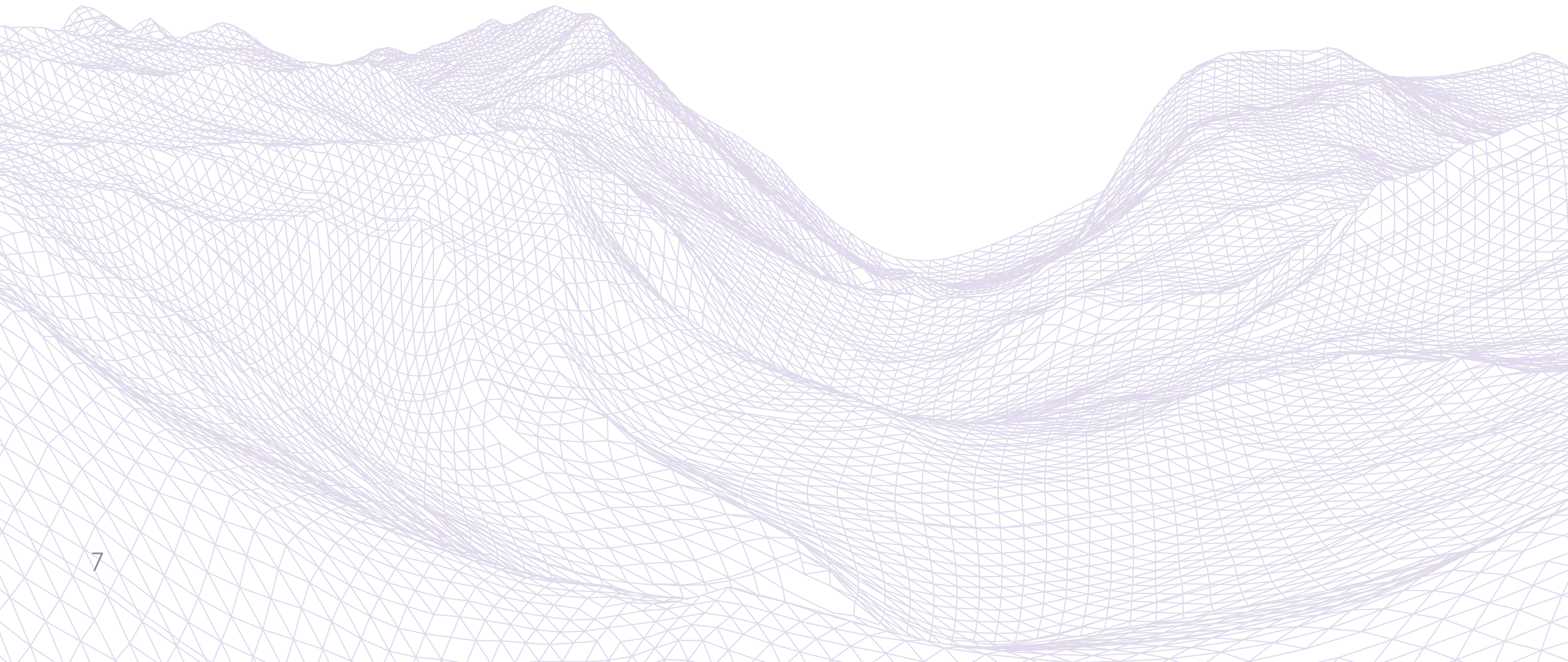
> **CUJO AI is here to help network service providers that want to use privacy-first solutions for large scale device statistics and model detection without relying on MAC addresses.**

What This Means for Network Operators and the Overall Online Experience

Many network operators rely on MAC addresses to identify devices and device types in their networks for traffic steering, policy management, and customer service. Some vendors use MAC addresses for 2 factor authentication or as a unique identifier for public hotspots and networks using multiple SSIDs. Random MAC addresses make these solutions obsolete:

- Network operators **lose usage histories** attributed to MAC addresses.
- **Wi-Fi steering** via MAC addresses **becomes unreliable**.
- **Users are forced to re-authenticate every time** they connect to another router or band (2.4 or 5 GHz).
- MAC-based public Wi-Fi authentication **no longer works** in hotels, universities, and other public hotspots.

MAC randomization will impact seamless authentication solutions based on MAC addresses; therefore many users might be forced to re-login or re-authenticate and update device policies constantly.



2 Questions Every Network Service Provider (NSP) Must Ask Itself

Here is a simple two-step process for determining whether MAC randomization will impact an NSP:

1. **Do you have any systems, services or platforms that use MAC addresses of consumer devices?**

2. **If you do, does it use MAC addresses as unique identifiers for record keeping?**

How Is CUJO AI Addressing Randomization?

CUJO AI has resolved the complicated issue of identifying devices without the use of MAC addresses and recently filed a patent for an industry-leading device intelligence solution that analyzes more than a dozen data points from a device connection's metadata. In under 5 minutes CUJO AI can identify, classify and merge records of devices with randomized MAC addresses, making usage history, traffic steering and network management accessible to network operators without using a device's MAC address. This solution is 100% privacy-respecting.

What Can CUJO AI Do Without MAC Addresses?

Our patented AI-driven Device Intelligence solution uses privacy-respecting metadata analysis and device identification that helps major network service providers:

- Respect their end-user privacy and protect their identity.
- Link and merge device signatures that have randomized their MAC addresses.
- Merge historical usage records of a device that uses multiple MAC addresses on different SSIDs.
- Deliver proven device-specific identification accuracy of over 74% in the first minute.
- Bring the total identification rate to over 92% in the first 24 hours.
- Do all of this without relying on MAC addresses or other unreliable information, as our machine learning algorithms analyze multiple data points for extremely high precision to identify over 50,000 unique device and OS types.

> **CUJO AI's Device Intelligence works as a cloud computing solution, therefore end users do not have to install any additional software. The NSP owns all network data. CUJO AI is also working on a Phase 2 Device Intelligence solution that has shown even higher accuracy and speed during tests. It is set for release to production by the end of 2020.**

CUJO AI

CUJO AI is the global leader in the developmentand application of artificial intelligence to improve the security, control and privacy of connected devices in homes and businesses.

CUJO AI brings to fixed network, mobile and public Wi-Fi operators around the world a complete portfolio of products to provide users with a seamlessly integrated suite of Digital Life Protection services while improving their own network monitoring, intelligence and protection capabilities.

More information: **connect@cujo.com**

Media inquiries: **press@cujo.com**

cujo.com