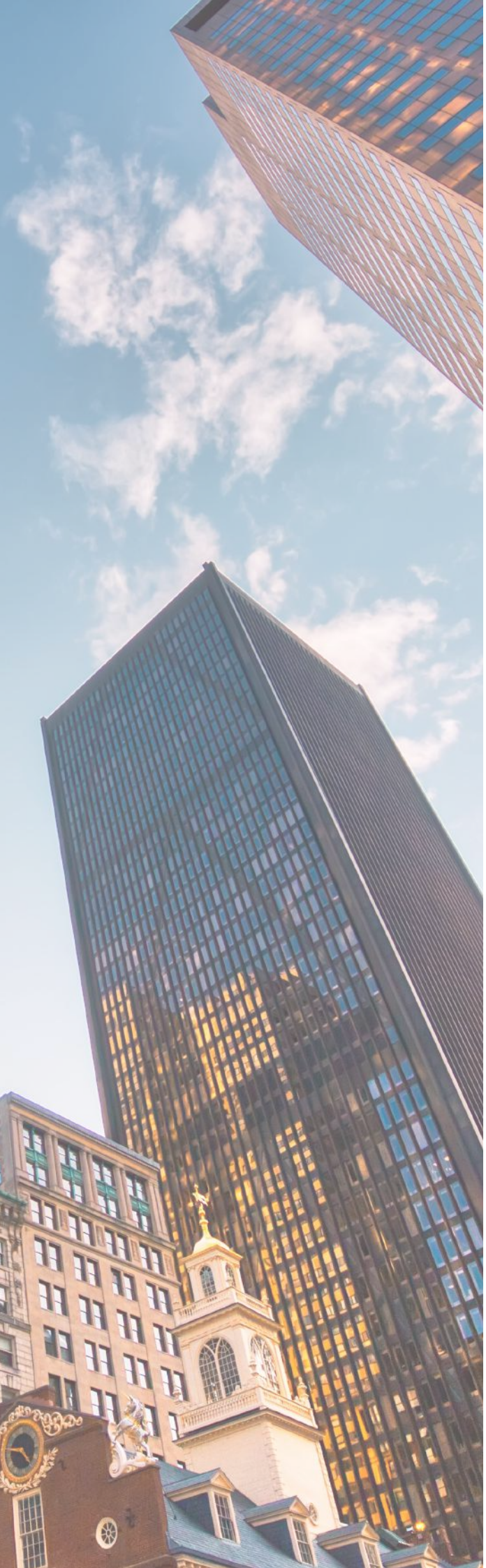
globalreach

The Implications of MAC Randomisation on Your Wi-Fi User Experience



BACKGROUND

A Media Access Control (MAC) address is a unique identifier associated with the specific network hardware within the device itself. This MAC address is used for the identification, management and authentication of individual devices wherever they connect or move around.

Apple will be introducing a new 'Private Wi-Fi' feature (a form of MAC randomisation) with iOS14, which will most likely happen from September. This is set to have major implications on the Wi-Fi user experience.

WHAT IS CHANGING?

More and more devices are being updated to be more secure to protect Personally Identifiable Information (PII) and user privacy and block the ability of service providers to track users.

One such security solution that has been rolled out by device manufacturers like Google, Microsoft and others over the past year has been the use of a locally generated random MAC address each time a device communicates with a new wireless network. Once connected to that wireless network, devices use a set MAC address each time a connection is made to that network.

While recently announcing its forthcoming operating system which is expected to ship in September 2020, Apple stated that it would be implementing a similar randomisation feature, which it refers to as "Private Wi-Fi'" addresses.

An excerpt from its statement says:

> "To further protect your privacy, your iPhone, iPad, iPod touch, or Apple Watch can use a different MAC address with each Wi-Fi network.
>
> To communicate with a Wi-Fi network, a device must identify itself to the network using a unique network address called a media access control (MAC) address. If the device always uses the same Wi-Fi MAC address across all networks, network operators and other network observers can more easily relate that address to the device's network activity and location over time. This allows a kind of user tracking or profiling, and it applies to all devices on all Wi-Fi networks.

> To reduce this privacy risk, iOS 14, iPadOS 14, and watchOS 7 use a different MAC address for each Wi-Fi network. This unique, static MAC address is your device's private Wi-Fi address for that network only."

While users can manually switch this function off through their settings, the current intention is to release the update with the function on all devices by default.

THE IMPLICATIONS FOR VENUES AND THEIR USERS?

Visitor-based networks usually require some form of authentication, or at least acceptance of terms and conditions. In many cases, the MAC address is currently used as the unique identifier for a device.

The new change by Apple iOS 14 means that after upgrading, a user's device will regenerate a new private MAC address, requiring a user to register or re-accept terms and conditions for access. This may skew statistics in the first couple of months as all iOS14 devices will appear as new subscribers.

Policies that limit the number of devices that can connect in an area, and rely on the MAC address may no longer be accurate as a single device can connect with a new private MAC address after upgrading.

Some venues use the MAC address to recognise devices of loyalty programme members or VIPs. Other authentication methods will be needed to identify these users.

Clearly this also affects reporting based on MAC addresses.

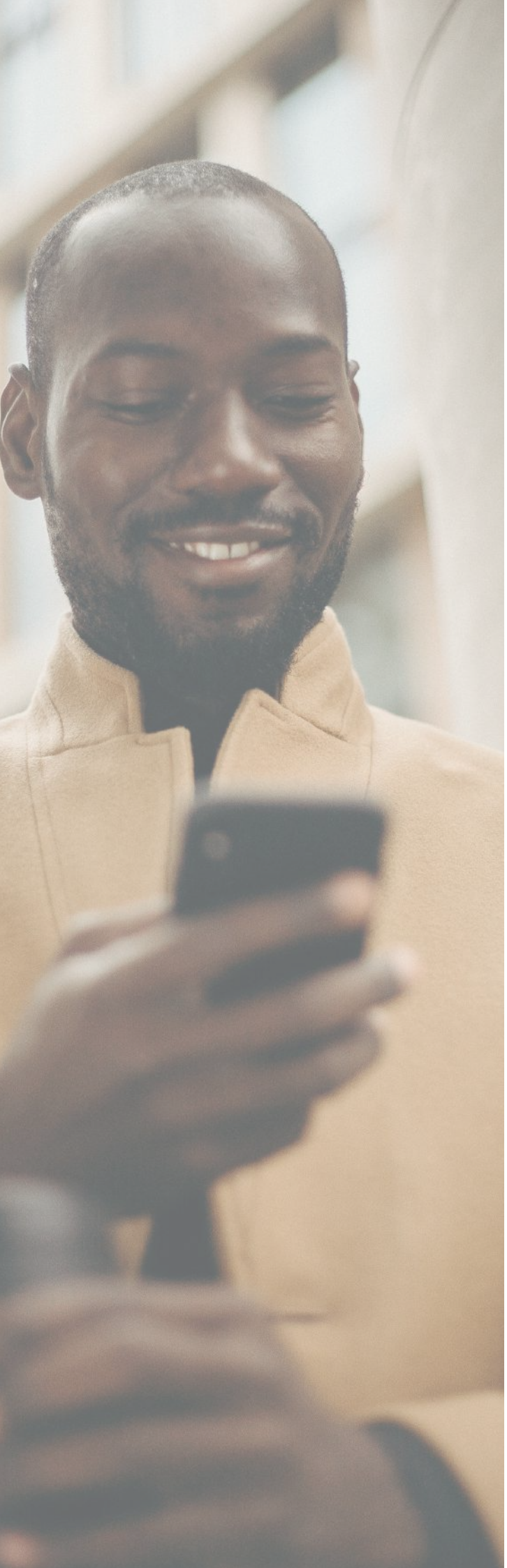
WHAT ARE THE OPTIONS?

There are several options open to venues and enterprises to eliminate or minimise the impact of MAC randomisation:

- Ask users to turn off the Private Address feature
- Modify internet service offerings
- Enable alternative authentication methods
- Passpoint (Hotspot 2.0)

Each option provides various benefits and trade-offs for venues and their users.

	Passpoint Enable	Alternative Authentication Methods Enabled	Modify Internet Service Offerings Modified With 24 Hour Limit	Request Users Disable Private Addresses
Present Property Portal for Initial Connection	YES	YES	YES	YES
Require Users to Authentiate Again After 24 Hours	NO	YES	YES	NO
Retain All User Entitlements After 24 Hours	YES	YES	NO	YES
Enable Automatic Vip Access	YES	NO	NO	YES
User Experience	A+	A	B	C
User Devices Supported	Almost All	All	All	Some



Passpoint (Hotspot 2.0)

Currently the best option is to implement the use of a Passpoint experience, on any network and device that can support it. Having a Passpoint profile on the device and enabled on the wireless network on-site allows for seamless secure authentication and management of the network and decouples the identity of the device from the MAC address which can no longer be counted on to remain static.

To use Passpoint, a profile must be installed on the device, directly or via an app, and enabled at the venue. GlobalReach Technology, is a proven leader in Passpoint Hotspot 2.0 implementation and delivery, with an industry-leading Online Signup Server (OSU) for easy device onboarding that is compatible with all major operating systems.

Passpoint is supported by almost all current devices and is a mature standard and offers the best option for seamless and secure access. Passpoint will also future proof your service and offers the prospect of enhanced roaming capabilities, as it is a requirement for the OpenRoaming Federation. However, in the few cases where older, incompatible devices or networks are not supported, and where an upgrade is not seen as an option, one of the following short term options solutions listed below will need to be explored.

Alternative Authentication Methods

Implementing alternative methods of authentication allows internet access purchases and entitlements such as loyalty programme benefits and bandwidth upgrades to persist if a user is at a venue for longer than 24 hours. With user authentication, the new MAC address associated with the device can also be associated with the user and the appropriate access privileges enabled.

Examples of potential authentication options include vouchers, PMS, or other authentication that is tied to an entry, like a username password pair, that the user can enter for all the different devices or device identities when the MAC address changes. In this scenario however, there can be no limit to the number of devices that can be linked to the authentication.

With this option, users may still need to authenticate in the future if Apple implements a time-based private MAC

However, loyalty programme benefits, bandwidth upgrades and other entitlements would be maintained over the entire duration of a user's visit.

All devices would be supported with this approach.

Turn Off the Private Address Feature

Customer and employee devices running Apple iOS 14 or above have the option of disabling the Private Address feature for the site's specific wireless network within their setting app.

With this feature turned off, MAC addresses of customer and employee devices would not change over the duration of the connection. This consistent MAC address would allow access to the wireless network for as long as the authentication Permits.

However, users may have concerns about the privacy and security implications of disabling this feature. These concerns are amplified by the security warning that appears on a device with this feature disabled. Because it is unclear how many users with Apple devices would agree to turning off this feature, this option cannot be counted on to provide a solution for everyone.

You can stop or resume using Private Addresses on an iPhone, iPad, or iPod touch running iOS 14:

1. Open the Settings app, then tap Wi-Fi.
2. Tap the information button ⓘ next to a network.
3. Tap Use Private Address. If your device joined the network without using a private address, a privacy warning explains why.
4. The new setting is used the next time your device joins the network. If you want to use it immediately, turn Wi-Fi off and back on in Control Center or Settings, then join the network.

NEXT STEPS

GlobalReach Technology is here to help you navigate this important change.

We welcome the opportunity to discuss the best option for your Wi-Fi service: **sales@globalreachtech.com**

globalreach

sales@globalreachtech.com
+ 44 20 7831 5630