

ARTICLE 19 Liaison Statement to Wireless Broadband Alliance in relation to MAC randomisation

Abstract

This document contains responses to the concerns raised by Wireless Broadband Alliance members in its liaison statement to ARTICLE 19 on 4 September 2018, regarding recent developments at the The Institute of Electrical and Electronics Engineers (IEEE) 802.11 working group (WG) on randomisation of MAC (media access control) addresses with the purpose of protecting client device owners' privacy and security (802.11aq amendment).

Introduction: MAC addresses and privacy

The use of MAC addresses as unique identifiers for owners and users of devices with wireless capabilities has been demonstrated to negatively impact their right to privacy and identity.¹ By facilitating tracking of these individuals' movements, or interfering with their private collection of news and other information, MAC addresses have contributed to infringements to the inviolable right to self-determination.² ARTICLE 19 considers privacy and freedom of expression to be mutually reinforcing³ and we see benefits in bringing functionalities to devices with wireless communications that put more control over user data in the hands of users.

As such we welcome recent developments in IEEE 802 LAN/MAN Standards Committee (LMSC) to standardize the randomisation of MAC addresses. The new features solve to real privacy problems identified in research⁴ and mitigating increasing concerns about vulnerability to privacy risks.⁵

¹ Mathieu Cunche, I know your MAC address: targeted tracking of individual using Wi-Fi, J Comput Virol Hack Tech (2014) 10: 219.

² Datainspektionen, 31702-2015, *Tillsyn enligt personuppgiftslagen (1998:204) av Västerås Citysamverkan AB*; Autoriteit Persoongegevens, z2014-00944, *Wifi-tracking van mobiele apparaten in en rond winkels door Bluetrace*.

³ ARTICLE 19, The Global Principles on Protection of Freedom of Expression and Privacy, 9 March 2017.

⁴ Jeremy Martin*, Travis Mayberry, Collin Donahue, Lucas Foppe, Lamont Brown, Chadwick Riggins, Erik C. Rye, and Dane Brown, *A Study of MAC Address Randomization in Mobile Devices and When it Fails*, Proceedings on Privacy Enhancing Technologies ; 2017 (4):268-286.

⁵ See e.g. DMA, *Data privacy: What the consumer really thinks*, February 2018 (survey of the UK public) or Insight Intelligence, *Delade meningar 2018* (survey of Swedish individuals), but also J. Turow, M. Hennessy, and N. Draper, *The tradeoff fallacy*, 2015, or L. Rainie, S. Kiesler, R. Kang, M. Madden, M. Duggan, S. Brown, and L. Dabbish, *Anonymity, privacy, and security online*, Pew Internet & American Life Project, 2013.

We understand that the recently introduced MAC randomisation features facilitate compliance with existing regulatory requirements for wireless communications network deployment in some European jurisdictions and expect similar regulatory compliance benefits to arise in an increasing number of jurisdictions as data protection legislation becomes more widespread.⁶

User transparency challenges with MAC address identification

Using a device's MAC address to uniquely identify and track, trace or monitor the behaviour of an individual user is inherently a problem of transparency. While a MAC address can be changed or randomised by a sufficiently knowledgeable user, for most private persons a device's uniquely assigned MAC address is an obscure part of their technical device that they likely do not understand is being used to map their movements and behaviour. For this reason, leveraging technical mechanisms to protect the individual's privacy from such unexpected tracking is important.

This opacity is raised by the WBA: access points and service providers track the history of devices that have connected. While the WBA proposes that MAC randomisation bloats such records, ARTICLE 19 would argue that it is an obscure form of tracking that is probably not well-understood by the customers of WBA members. The benefits of transparency for the consumer outweigh the benefits WBA members may gain from smaller logs.

MAC randomisation is effectively already in use

MAC randomisation is effectively already implemented for the most common types of consumer devices today through the device's operating system rather than at the chip hardware level.⁷

ARTICLE 19 argues that MAC randomisation is not new, and should not come as a surprise to WBA members. The already wide-spread deployment of this feature speaks against WBA concerns about MAC duplication, collisions, parental controls and blocklisting. It would be surprising if WBA member customer help services had not already effectively established processes and protocols to handle devices that employ MAC randomisation.

MAC randomisation settings

The IEEE 802.11aq amendment to the IEEE 802.11-2016 standard includes optionality. MAC randomisation is a feature that can be deactivated, and as such, ARTICLE 19 feels confident that WBA members will deactivate the

⁶ Cf. the Indian *Privacy Act* or the Brazilian *Lei Geral de Proteção de Dados Pessoais*.

⁷ *Supra* 4.

feature for its access point user stations (AP-STA). This should be helpful for WBA members' customer support when trouble-shooting.

Individual users who consent to being tracked and traced may also deactivate the MAC randomisation feature. However, a service should not request generation or collection of more unique identifiers pertaining to an individual than what is necessary for the provision of that service.⁸

Passpoint challenges

The Calling-Station-ID attribute of the RADIUS Access-Request Attributes in Section 2.1 of the Passpoint specification does not mandate, but does recommend using MAC addresses as a Calling-Station-ID. However, the recommendation is made with reference to the outdated RFC3580, which has since been replaced by RFC7268.⁹ The more recent RFC does not mandate tying of a Calling-Station-ID to a MAC address.

In the Passpoint specification we have reviewed (Wi-Fi CERTIFIED Passpoint(TM) (Release 2) Operator Best Practices (OBP) for AAA Interface Deployment, Version 3.0), maintaining a stable MAC address does not appear to be required across multiple access points, network names (SSIDs) or even within a singular SSID (although this wouldn't be covered by the 802.11aq amendment since it stabilizes the MAC address once association is made).

MAC identifiers and business models

Several of the concerns raised by the WBA Testing & Interoperability Workgroup are related to current business models. ARTICLE19 suggests revising these business models to better reflect modern technical and organisational privacy requirements on electronic communications services. MAC-based identification methods should not be used by wireless communications providers, for instance in short-term complimentary services or with respect to billing.

Moving forward with Chargeable-User-Identity (CUI) seems reasonable, not the least in the context of more or less privacy-friendly deployments already being in use in the popular educational wireless networks of the *eduroam* family.¹⁰ The WBA community may wish to explore modern authentication protocols, such as RADIUS-with-TLS or DIAMETER.¹¹

⁸ The principle of *data minimization* is enshrined in EU, Indian and Brazilian data protection law, as well as being recognized as a good information security mechanism and privacy by default mechanism. See e.g. RFC6973 *Privacy Considerations for Internet Protocols*, IEEE P802E *Privacy Recommendations* draft 1.1 or ENISA, *Privacy and Data Protection by Design*, January 12, 2015.

⁹ IETF RFC7268, *RADIUS Attributes for IEEE 802 Networks*.

¹⁰ IETF RFC7593, *The eduroam Architecture for Network Roaming*.

¹¹ *Ibid.*, section 4.1.


Regulatory requirements: traceability and lawful intercept

Because of the ease with which MAC addresses can be spoofed by technologically skilled users, it is challenging for ARTICLE 19 to see why compliance with the regulatory mechanisms brought up by WBA members would be compromised by introducing MAC randomisation mechanisms in the IEEE 802.11 standard.

Conclusion

In conclusion, ARTICLE19 understands the MAC randomisation feature introduced in the 802.11aq amendment to be a necessary, but insufficient, step on the way towards enhancing robust privacy protection for all technology users, not just those users who are technically savvy.

Privacy by design and by default is a welcome development, and should be seen as such in the WBA community. We stand ready to engage further with the WBA community on this topic, and the topics covered above.



Thomas Hughes

Executive Director

ABOUT ARTICLE19

ARTICLE 19 is an international human rights organisation, founded in 1987, which defends and promotes freedom of expression and right to information worldwide. It takes its mandate from the Universal Declaration of Human Rights, which guarantees the right to freedom of expression and information.

An increasingly important means of expression and to seek, receive, and impart information is through information and communication technologies such as the Internet. ARTICLE 19 has been promoting Internet freedoms for over 10 years and is active in developments of policy and practice concerning freedom of expression and the Internet through our network of partners, associates and expert contacts.