Wi-Fi Privacy and Security: Evolving to Keep up with Marketplace Demands

A Technical Paper prepared for SCTE by

Carol Ansley
Lead Architect
Cox Communications, Inc.
Carol.ansley@cox.com

Tushar Sharma
Lead Network Engineer
Cox Communications, Inc.
Tushar.sharma@cox.com

Table of Contents

Title **Page Number**

1. Introduction

When Wi-Fi™ was first developed over twenty-five years ago, no one expected that it would become the dominant method of connecting consumer mobile devices into the larger network wherever people went. The past 10 years have seen Wi-Fi connected mobile devices go from a business convenience to a personal and professional necessity. More recently consumers using Wi-Fi mobile devices have become aware that their privacy was being impacted by these ubiquitous devices. A person could be tracked by the mobile devices they carried as they worked, shopped, and traveled. The privacy concerns associated with Wi-Fi have been written about in many papers. Information exposed in Wi-Fi headers and unencrypted control frames have been highlighted as providing a window for third parties to monitor and track users through their mobile devices.

IEEE 802.11™ first addressed these concerns with IEEE Std 802.11aq™ that recommended various steps such as randomizing a mobile device's MAC address to obfuscate the user's identity. The consumer electronics industry has enthusiastically adopted this recommendation which ended up having ripple effects in other areas. We discuss possible mechanisms to reduce the effect of randomized MAC address that are being considered by the Random and Changing MAC Address Operation Task Group in IEEE 802.11.

We will discuss ongoing work in 802.11 including proposed protocol changes that are being considered within IEEE 802.11 such as the work being done by the Enhanced Data Privacy Task Group in IEEE 802.11. The task group is developing new tools to reduce the ability of a third party observer to identify and track Wi-Fi mobile devices, and the users associated with them.

We also provide some references in the *Bibliography and References* section for further reading on similar efforts in the 3GPP Standards. Such references are not exhaustive but suggested literature.

2. Terminology

2.1. Privacy Terminology

Since we are covering different aspects of privacy in this paper, agreement on common terminology is useful. Privacy experts have developed categories for information to indicate its relevance to privacy concerns. Within the Recommended Practice for Privacy Considerations for IEEE 802 Technologies (IEEE Std. 802E-2020), these definitions below are useful to consider as we discuss potential improvements to Wi-Fi protocols.

- *Personally Identifiable Information (PII)* – Any data that directly or indirectly identifies a person or from which the identity or the contact information of a person can be derived.
- *Personally Correlated Information (PCI)* – Data gathered about an identified person or small group of people by observing activities (e.g., communications) or events associated with those people.
- *Personal device* – a device associated with a person or a group of users, such that identification of the device also allows identification of its user or group of users.

In the sections that follow, mobile devices will be discussed with the assumption that these devices are personal devices. For example, a smartphone is a common personal device. People rarely share smartphones with others, and commonly carry them wherever they go.

The information discussed later in connection with Wi-Fi standards activities will be mentioned as PCI, where it allows data to be correlated with certain people or groups of people, and PII, when it allows data to identify, usually indirectly, a specific personal device and the device's user.

2.2. Wi-Fi Terminology

Wi-Fi also has a lot of terminology specific to its technology. A Wi-Fi system generally consists of an Access Point (AP) which is a unit with a connection into a wider network, usually a wired network, and a Wi-Fi radio interface. Connecting on that radio interface are stations, which are usually mobile devices using the AP to reach the wider network.

When a mobile device such as a smartphone establishes a connection to an AP, that process is called associating with the AP. At the same time the mobile device can also authenticate itself to the AP and the wider network in a security association. If a mobile device moves out of range of an AP, the AP generally will consider the device to have de-associated and will require the device to go through the authentication and association processes again to rejoin the network when the device returns to the AP's wireless range.

A mobile device determines which APs are in range by sending out Probe Request messages. These messages ask for APs to return Probe Response messages that contain information about their services. Similarly, Association Request and Association Response messages are used by mobile devices to request an association with an AP and by the AP to respond to that request, respectively.

3. Wi-Fi Privacy and Security Standards Activity

Wi-Fi standards originate from both the IEEE Standards Association and the Wi-Fi Alliance. In this section, we are discussing IEEE SA standards activity.

Due to a lack of a standardized device identifier, an IEEE MAC Address has become the *de facto* identifier for devices and by extension their users. However, this identifier lacks Security and Privacy constructs that have become increasingly important to users. For instance, a device can start using a MAC address that it created randomly. If it wants to impersonate another device at the MAC level, it just has to start using the MAC address of that other device.

Additionally, the 802.11 protocols did not initially focus on minimizing exposure of identifiable parameters, like the MAC address, to third party observers. Additional parameters shared openly in messages such as a Probe Request or Association Request message may also allow a mobile device's activities to be correlated with specific targets, and by extension may expose PCI or PII of the device's user.

A deeper dive into MAC randomization and other related Wi-Fi topics are discussed below. MAC Randomization enhances privacy and security but complicates the customer experience and network management since device OEMs have varied implementations. From a broader perspective, within the current generation of 802.11 protocols, a mobile device's MAC address is expected to remain stable while the device is associated with an AP. This continued use of a single MAC address allows tracking of a mobile device and its user. The discussion below will address this use case and ideas that are under discussion to reduce the exposure of PCI, such as a personal device's location. Finally, Open SSIDs typically use the MAC Address as a mobile device identifier and any subsequent changes to this identifier are treated as a new mobile device complicating Customer Experience. A discussion of potential impacts to existing operational functionality are covered in a discussion below of the privacy challenges associated with Open SSID.

3.1. Random and Changing MAC Addresses

3.1.1. What is a MAC address?

For those who have spent a lot of time in this area, the authors invite you to skip ahead to the next section. But if you are curious, a Medium Access Control address, or MAC address, was originally developed to be able to distinguish one device from the next on a network. The MAC addresses in Ethernet headers allow a device to determine if an incoming message is addressed to it, for example, by matching the MAC address in the header of an incoming message with the device's MAC address. MAC addresses are also extensively used in the IP networking protocols for mapping IP Addresses to individual network interfaces on network infrastructure entities, such as DHCP servers.

The most common 48-bit MAC addresses consist of 12 hexadecimal digits with 2 bits indicating whether the MAC address is a unicast or multicast address and whether it can be expected to be globally unique or if it is locally administered. The IEEE Registration Authority developed a system of assignment for the first 3 octets of the MAC address. An equipment provider can purchase an allotment of MAC addresses so that its devices can be programmed with unique hardware MAC addresses.

3.1.2. MAC Addresses and Wi-Fi

The networks using MAC addresses were originally wired, of course, but the concept of using a MAC address to uniquely identify devices was brought into the development of wireless networking as well. Within the protocols of 802.11, MAC addresses are used extensively. For example, MAC addresses can identify the source and destination devices for each transmission in the header fields of that transmission.

As people began using more Wi-Fi enabled mobile devices, particularly smartphones, eventually industry began to equate the presence of a user with the presence of their mobile device. A personal device's MAC address became PCI and PII. Features assuming this linkage allowed simplifications in the user experience. For example, a user might log in once to an in-house system using their personal device, then the system would recognize that user by their mobile device MAC address when they returned, and not require the user to log in again. Over time, the use of MAC addresses to provide permanent identifiers was converted into a way for outside observers to track the movements of mobile device users, as well as to analyze their traffic. A user's path through a store could be mapped and advertisements adjusted to target their perceived interests. An employee's location in an office or warehouse could be tracked minute by minute. Privacy advocates began writing about this exposure and the industry began experimenting with options to increase people's privacy.

802.11 analyzed this problem in 802.11aq and added recommendations to the 802.11 standard. The potential use of randomized MAC addresses was discussed in that amendment along with other enhancements intended to increase the difficulty of tracking a particular mobile device. Packet sequence numbers and scrambler seeds can also offer an observer the ability to track a mobile device. Changing those values when the MAC address changes can make it more challenging for a remote observer to associate one packet with an old parameter set to another using a new random set of parameters.

The Wi-Fi mobile device industry began to implement MAC randomization to address consumer privacy concerns. The difficulty with MAC randomization was that if a mobile device presented its access point with a new MAC address after the authentication and association process was complete, the association with the access point would drop and the mobile device would need to go through the association process again. This re-association tended to interrupt traffic flows and could cause a user to be asked to reauthenticate with the system behind the access point since, to the access point, an entirely new mobile

device had suddenly appeared. Resulting from this observation, most devices utilizing MAC randomization did not change their MAC addresses while associated to an access point.

Because there was not a standardized overall solution, different vendors implemented MAC address randomization in different ways. One common implementation choice was to allow the mobile device to store a record of which MAC address it had last used with an access point and return to using that MAC address when the mobile device determined that it had returned to that access point. While this feature did reduce somewhat the ability of the third-party tracker to connect the mobile device's user across multiple unrelated access points, it did not help with a user who returned to the same coffee shop, for example. Another common implementation choice was to direct the mobile device to change its MAC address and associated parameters on a regular cadence of hours or days. A user would experience the need to log in to systems more often, but from one day to the next, a third party might have difficulty linking the user's activities.

3.2. Additional Corelatable Information with Wi-Fi

In addition to the MAC address, Wi-Fi devices can communicate a lot of information when they are searching for a new connection and while they are connected to an access point. In a Probe Request or an Association Request, a mobile device can include configuration information aside from just its MAC address. The purpose of the extra information was to allow the access point to potentially provide additional features to the mobile device, or more efficiently direct it to a radio band that might best suit its capabilities. But these assortments of device parameters and user configuration choices effectively have given an observer the ability to fingerprint a mobile device. That device fingerprint can provide at least PCI and, in some cases, PII about the user of a mobile device.

For example, one parameter a mobile device can include is the SSID of its preferred access point. Setting this parameter to a user's home access point's SSID allows an observer to know that that mobile device is at least connected to that user, if not a mobile device carried by that user as a personal device.

3.3. Current 802.11 Task Group Activities

802.11 has returned to the topic of MAC privacy enhancements to consider improvements in this area. A technical interest group or TIG was formed in May 2019 to consider whether the randomized and changing MAC addresses appearing in the field presented an issue that 802.11 should investigate in more detail. The TIG became a study group in 2020 that developed statements of work for two new task groups. 802.11 Task Group bh, TGbh, was formed to develop an amendment with updates to 802.11 that can address some of the problems created by RCM without significantly damaging the improved privacy that it offers users. 802.11 Task Group bi, TGbi, was formed to consider improvements to user data privacy within 802.11 more broadly in a separate amendment to the standard.

Within the IEEE standards development structure, a standard is managed by a Working Group. The 802.11 Working Group works on the standard for Wi-Fi. New amendments to the standard are developed in task groups at the behest of the working group. By inaugurating two new task groups, the 802.11 Working Group recognized that additional standards work in this area would have benefits for the standard and its user community.

3.3.1. TGbh - Operation with Randomized and Changing MAC Addresses

The identified scope for TGbh included preserving "the ability to provide customer support, conduct network diagnostics and troubleshooting, and detect mobile device arrival in a trusted environment." All

of these features had been degraded or rendered unreliable by the implementation of randomized MAC addresses on mobile devices.

When a user has been experiencing difficulties with a mobile device that has RCM active, a customer support agent might not be able to link any records of association difficulties or other problems to the problematic mobile device since the AP records might reflect an assortment of MAC addresses. Similarly, many networks track mobile devices by their MAC addresses. As RCM was deployed, often without a user even realizing it, the number of MAC addresses appeared to multiply exponentially. For access points that limited the number of allowed MAC addresses, they began to experience customer complaints when the mobile devices using RCM were no longer allowed to connect. Finally, complaints also came in from users who expected their mobile devices to be recognized by a trusted home or office environment. Instead of the seamless connection experience they had experienced previously, the users were required to log in every time they returned to associate to a well-known system.

TGbh has been developing mechanisms compatible with present networking methodologies that will help improve the performance of networks with mobile devices using RCM. The task group's challenge is how to enable a mobile device to share information securely with an access point that will allow the access point to recognize, to a lesser or greater extent, the mobile device without exposing the user to reduced privacy. An important part of the discussion has dealt with the tradeoffs facing a user. A straightforward decision must be made by the user whether to allow the network represented by the access point knowledge of the mobile device's identity or at least whether it has associated with this access point in the past. Emphasis has been placed on efforts to retain as much of the RCM privacy enhancements as possible to reduce the user's exposure to third party trackers while allowing a mobile device to expose additional information to the access point for improved user experiences. The information may be as simple as providing information from a mobile device to allow an access point to connect that newly associated mobile device with a mobile device that had a different MAC address when it associated with the access point in the past.

TGbh has also considered whether an access point should be able to recognize a returning mobile device during the association process, or if it is sufficient to recognize the device after it has associated. The ability to recognize a returning mobile device during the association process enables additional features, such as the ability to steer a mobile device to a favored band for association. On the other hand, for an access point to recognize the mobile device before association, some parameters must be passed before encryption is in place. The pre-association feature thus must be carefully designed to ensure that it does not increase the privacy risk.

For all of the possible TGbh features, similar to the current RCM features, Wi-Fi device manufacturers and software developers will have to decide the level of involvement of the end user. Will features default to enabled or disabled, for example.

The current timeline for TGbh predicts that its amendment may issue through IEEE SA in September of 2024.

3.3.2. TGbi – Enhanced Service with Data Privacy Protection

When 802.11 decided to investigate improvements in user privacy, TGbi was launched in parallel to TGbh with the scope of specifying "new mechanisms that address and improve user privacy." The task group was started in view of the need for standardized mechanisms to improve protection for users of Wi-Fi enabled mobile devices against user tracking and user profiling.

TGbi began by considering different use cases and issues that related to user privacy. The group identified issues such as the ability of third party observers to track a user while the user's mobile device is associated, since the device cannot change its MAC address while associated without causing a full reassociation to be required. The task group also considered proposals for reducing information exposure in other actions that a mobile device might take, such as a location (PASN) session or a channel sounding. The suggestions of earlier amendments, such as TGaq, were also considered and expanded upon. For example, a mobile device seeking to find a new AP might send out a Probe Request that currently might include a lot of information that could be used to fingerprint the mobile device in later Probe Requests. TGbi is considering how to reduce messages such as a Probe Request to a bare minimum to also reduce the amount of information exposed to third parties.

TGbi has also been discussing possible improvements to AP privacy and security, particularly in connection to a mobile device used as a hot spot. A user might want to enable their mobile device as a hot spot to support other local mobile devices, but still want to minimize the information a third party could gather while the hot spot is active. Similar to minimizing content in a Probe Request, an AP using TGbi privacy mechanisms might restrict the amount of information it discloses to requesting mobile devices. The group is considering a new layer of encryption for some AP services that might further reduce the exposure of an AP to outside observers. Additionally, these features may also provide an additional layer of security to prevent AP spoofing, where a rogue AP is set up to capture traffic from mobile devices by using the SSID and other information from a trusted AP.

The current timeline for TGbi predicts that its amendment may issue through IEEE SA in March of 2026.

3.3.3. Overlap between TGbh and TGbi

The two task groups overlap in that they are both considering privacy related topics, but are distinct in that they have different focuses. TGbh is tightly focused on enabling mechanisms that allow a mobile device to be recognized by an AP when it returns to that AP, ideally with the continued use of randomized MAC addresses to maintain the user's privacy to third party observation. The mechanisms are all designed to allow the mobile device to implement them or not as instructed by a user or user provisioning. TGbi is more broadly considering methods of expanding the anonymity of a mobile device as it interacts with access points both before and after association.

Once both task groups have completed their work, a Wi-Fi device might implement mechanisms from both eventual amendments. It might use a mechanism from TGbh to allow an access point to recognize it when it returns to reassociate, and it might use a mechanism from TGbi to continue changing its over the air MAC address while associated to that same access point.

4. Wi-Fi Privacy and Security Use Cases

This section discusses particular use cases that provide examples of Wi-Fi Privacy and Security developments.

4.1. Mobile device not recognized due to RCM

The use of RCM by mobile devices has resulted a number of unintended side effects that in many cases resulted from a mobile device not being recognized by an AP or network of APs because the new MAC address is not familiar to the AP(s). These use cases illustrate a couple of key scenarios.

4.1.1. Parental controls

Some parental control instantiations use mobile device MAC addresses to determine which rules to apply to a newly associated device. If the mobile device has RCM enabled, then it will probably not be recognized after its external MAC address changes. In some cases that may mean that the mobile device is only allowed to reach a walled garden of targets, in other versions, it might mean that the mobile device has no rules attached to its browsing. To avoid this issue before TGbh finishes its work, the user may be instructed to disable RCM on the mobile device. Alternatively, the user might be instructed to configure the mobile device to always use the same MAC address when associating with the local AP.

4.1.2. Help Desk interactions

In a commercial setting, a user may have a help desk that they can access when having connection problems with their mobile devices. The records the help desk can access may show several attempts of mobile devices to associate with the network, but with RCM enabled on a mobile device, each association attempt may use a different MAC address. The help desk technician can't tell which attempts are legitimate and which ones are suspect. To alleviate the issue currently, again the user must be instructed to disable RCM entirely, or to restrict it to a single MAC address for this AP.

It is important to note that the tactics noted above, disabling RCM or requiring reuse of MAC addresses for remembered APs, seem straightforward for technical professionals who are familiar with diving through technical menus and who already understand at least the basics of Wi-Fi operation. These directions can range from intimidating to extremely challenging for people who are non-technical or who are unfamiliar with the ins and outs of mobile device low level configuration. Because of this, most people tend to leave their mobile device settings on the device defaults. RCM spread most rapidly in the marketplace when mobile device vendors began to default their devices to enable RCM.

4.1.3. Changes planned in TGbh

The changes being discussed in TGbh are intended to allow a mobile device to identify itself to an AP with which it has previously associated to avoid the difficulties experienced currently.

In the parental controls use case, the mobile device might present an identifier to the AP after association. The AP could then compare that identifier to a previous record and determine the correct level of Internet access for that mobile device. The exchange of identifiers would be protected by the standard link level encryption of Wi-Fi, so a third part observer would not be able to glean the identifier through observation.

In the Help desk use case, the mobile device might use a random MAC address when it attempts association that has already be pre-shared with the AP in an earlier association. The pre-shared random MAC address would have been communicated in the previous association after a secure encrypted link was available to protect it from third party observation. Because the messaging request for association includes the declared MAC address of the requesting mobile device, the AP has the opportunity to identify the mobile device even before it has associated, thus allowing troubleshooting to occur even when or if the association fails.

4.1.4. Changes planned in TGbi

The changes under consideration for TGbi may present challenges for technical support in that the traditional fall back of capturing all the traffic on the air for later analysis may not be enough. As mentioned above, one of the TGbi's features is MAC address change while mobile devices are associated. For a complete analysis to be successful, a record of the MAC address transitions of the mobile devices

involved would be needed for the captured data to be useful. Alternatively, the AP and the mobile devices would need to be instructed to stop changing their MAC addresses for a time while the test is in progress.

4.2. User tracking by third party observers

The current behavior of Wi-Fi devices with or without RCM can expose user PII, such as location and activities. 802.11 currently does not allow a mobile device to change its MAC address over the air without a full reassociation. As mentioned earlier, current RCM implementations often use the same MAC address when returning to a known AP or network. As a result, with or without RCM the movements of a user though their mobile devices can be tracked while they are associated with an AP.

4.2.1. Smart Home

A smart home may have a mixture of fixed location and mobile Wi-Fi devices, where the fixed location Wi-Fi devices may be considered IoT devices. Generally, very few IoT devices use RCM features, though most do support encryption after association. Because of these fixed MAC addresses, even though an observer may not be able to decrypt the device transmissions, an observer may be able to determine that a particular MAC address is associated with lights or a door or a camera by simple observation. Once that pattern is known, an observer may be able to determine through remote monitoring of Wi-Fi frequencies when a person enters and leaves their home, for example. Similarly, if the person also carries a mobile device (a reasonable expectation), the observer may be able to associate the appearance of a particular MAC address with the presence of a particular person in the home.

4.2.2. Changes planned in TGbi

802.11 TGbi is considering new features that allow a device to change its over the air MAC address while associated with an AP. An external observer would record a set of MAC addresses that are changing and may not be able to determine without direct observation whether the changes represent actual new mobile devices or the existing mobile devices changing their MAC addresses. For a small set of devices, that problem might not be too complicated, but as the number of Wi-Fi enabled devices increases within the home and the number of channels available for those devices also increases, the problem of keeping track of how many devices are present rapidly becomes difficult to solve without statistical packet analysis or other more sophisticated efforts.

4.3. Open SSID and DMCA/CALEA

Open SSIDs have been used in the hospitality industry and other industries in conjunction with authentication services through Portals. The use of RCM can present issues if the user expects the portal behind the open SSID to recognize their mobile device and allow its services to be provided without incident. The use of RCM can also allow individuals who want to preserve their privacy for less savory means to hide their connection to particular locations or events.

4.3.1. DMCA with Open SSIDs

The DMCA was put in place to protect copyright owners from unlicensed use of their copyrighted content. The DMCA included specific provisions that copyright owners can use to enforce control over their content if it is used in an improper or unlicensed way.

Typical DMCA violations are captured using a public IP, date/time stamp and TCP/UDP port by the copyright owners. Based on the ownership information of an IP address, a Take Down Notice (TDN) is

generated and sent to the Service Provider associated with that IP address. The Service Provider maps this information back to a subscriber that was allocated the IP/Port combination. The mapping process uses the MAC address of the mobile device to ascertain the subscriber network information. Historical longevity and constancy of the MAC address allows this process to establish the Network identity using the MAC address as a correlation key. This relies on Usage Accounting information being provided by wireless gateways to analytic engines. Gateway Accounting information is not exposed to the AP and non-AP STA involved in RF communications.

Current MAC randomization methods are a compromise that may not easily comply with the need to support legal requirements under DMCA legislation. If a mobile device has RCM enabled without the feature of returning to the same MAC address at a given AP, it can be challenging to determine the actual device and to find the device's user to fulfill DMCA statutory requirements.

There are discussions of alternative identifiers that can be used to fulfill such requirements, which would allow MAC addresses to be no longer fixed – partially or fully. For example, RFC 4372 - Chargeable User Identity describes a solution capable of providing such capabilities, without the need for MAC address support.

Secure SSIDs can also leverage the same approach, or use other available identifiers which are PII and CPNI-friendly.

If TGbh features are enabled, then the access point may be able to associate repeat visits by the same device even if the over the air MAC address presented by the mobile device is changing between the visits. If the mobile device claims a different IP address on each visit, then the local AP or ESS network may be the only entity that can associate the different visits with a single device and user.

When TGbi privacy enhancements are rolled out, the privacy enhancements should only affect the ability of third party observers to track mobile devices. If the access point retains records of the devices associated, then the DMCA statutory compliance should be unaffected. If any system do rely upon third party observations of wireless traffic, they will be impeded by the changing of MAC addresses that will then occur even while the mobile device is associated.

4.3.2. CALEA/LI on Open SSIDs

The CALEA and Lawful Intercept legislation was put in place to provide support for law enforcement from telecommunications companies. CALEA/LI require support for wiretap capabilities on wireless networks. These capabilities typically use the MAC address of target mobile device in the Wi-Fi networks today.

On 3GPP networks, due to availability of other identifiers (IMSI – International Mobile Subscriber Identifier or its derivative identifiers), a MAC address is not necessary.

On a Wi-Fi network, the (3GPP) X1 interface (or equivalent) enables or disables the wiretap [typically] using a RADIUS Change-of-Authorization (CoA) request packet. The resulting control plane data is transferred to the LI Mediation Function over the (3GPP) X2 (or equivalent) interface. The tapped content is transferred to the LI Mediation Function via the (3GPP) X3 (or equivalent) interface.

If a device has RCM enabled, using the MAC address to identify a device and access its communications is no longer sufficient.

As noted in the previous section, alternative identifiers can be used to fulfill such requirements, which would allow MAC addresses to be no longer fixed – partially or fully.

Secure SSIDs can also leverage the same approach or use other available identifiers which are PII and CPNI-friendly.

Again, if TGbh features are enabled on the AP and the mobile device, then the visibility into the activities of a specific mobile device is improved. Even if it uses a different MAC address, the TGbh feature can allow the AP to associate that device back to information from previous associations.

When TGbi features are active, they should not interfere with CALEA/LI as long as those systems are not dependent upon the over the air MAC address. The AP and larger network will still be able to identify the device and capture its communications.

5. Conclusion

This paper provides a glimpse into privacy related activities in IEEE 802.11. The updates under consideration may affect operator companies over the next 2-5 years as the features roll out. The experiences of the past suggest that the rollout of new Wi-Fi features can be slow, but RCM has been an exception to that rule. It was not even standardized formally, but spread quickly through the Wi-Fi world driven by the consumer interest in improved privacy. As TGbh and TGbi work through the standardization process, operators should monitor their development and consider how to prepare their networks for these new features.

The work of the IEEE 802.11 task groups will continue for at least two years, so interested parties have a chance to reach out to the group if they have additional ideas to contribute. If you are interested in becoming involved in the standards development process, please let the authors of this paper know and we can provide additional information.

Note that all comments in this paper are the professional opinions of the authors based on experiences and research. The authors do not represent 3GPP, IEEE, 802, 802.11 or any of the 802.11 task groups in any capacity.

Abbreviations

AP	access point
CALEA	Communications Assistance for Law Enforcement Act
CPNI	customer private network information
DMCA	Digital Millennium Copyright Act
FEC	forward error correction
HD	high definition
IEEE	Institute of Electrical and Electronics Engineers
IOT	Internet of things
LI	legal intercept
MAC	medium access control
NE	Network Element
PII	personally identifiable information
RCM	random and changing MAC addresses
SCTE	Society of Cable Telecommunications Engineers
TIG	Technical Interest Group

Bibliography & References

Document Number	URL
Digital Millennium Copyright Act (DMCA)	The Digital Millennium Copyright Act
CALEA	Communications Assistance for Law Enforcement Act (CALEA)
Lawful Intercept (LI) – 3GPP	ETSI TS 103 221-1 V1.14.1 (2023-03) ETSI TS 103 221-2 V1.6.1 (2022-03) ETSI TS 101 671 V3.15.1 (2018-06)
WBA IMSI Privacy	WBA IMSI Privacy Standard v1.1
Android MAC Randomization	Android MAC Randomization Behavior
Apple MAC Randomization (iOS/iPadOS/watchOS)	Use private Wi-Fi addresses on iPhone, iPad, iPod touch, and Apple Watch
Customer Proprietary Network Information	Privacy/Data Security/Cybersecurity: Customer Proprietary Network Information
Personal Identifiable Information	Guidance on the Protection of Personal Identifiable Information
Task Group bh PAR	https://www.ieee802.org/11/PARs/P802.11bh.pdf
Task Group bi PAR	https://www.ieee802.org/11/PARs/P802.11bi.pdf
3GPP ITS Security	ETSI TS 102 941 - Intelligent Transport Systems (ITS); Security; Trust and Privacy Management; Release 2
3GPP Security Architecture	ETSI TS (1)33.501 – Security architecture and procedures for 5G System R17 (2022-05)

