COMMERCE SPECTRUM MANAGEMENT ADVISORY COMMITTEE (CSMAC)

Interference Prevention, Detection, and Resolution (IPDR) Subcommittee:

Mary Brown
Jeff Cohen
Thomas Dombrowsky
Dale Hatfield
Bruce Jacobs (NTIA Liaison)
Mark Lewellen
Jennifer Manner
Wayne Phoel
Carl Povelites
Andrew Roy
Mariam Sorond (co-chair)
Bryan Tramont (co-chair)

JULY 2020

Table of Contents

I. NTIA Question

NTIA has asked the CSMAC IPDR Subcommittee to address the following questions:

- How could NTIA's and the FCC's equipment authorization rules be modified to require that all transmitters use a unique identifier? What are the barriers to doing so?

II. Recommendations

The administrative path for modifying the FCC's and NTIA's equipment authorization rules to require that transmitters have a unique identifier – whether band-by-band or more broadly – appears to be straightforward. Although there are specific use cases where a unique identifier may be a viable and effective regulatory tool, the challenges with implementing any such a requirement on a ubiquitous basis would be complex and multifaceted. The Subcommittee recommends approaching the question of unique identifiers through a band-by-band or use case approach rather than some broader mandate in the equipment authorization rules.

III. Overview of FCC and NTIA Equipment Authorization Procedures

A. National Telecommunications and Information Administration

Operationally, the question of how the NTIA equipment authorization rules could be modified to require that RF transmitters transmit unique identifiers appears straightforward. The Assistant Secretary of Commerce for Communications and Information has the full authority to develop, set, and promulgate new rules for radio frequency (RF) transmitters deployed on federal radio frequencies.[1] Under this authority the Assistant Secretary, at his/her discretion, could modify existing rules to require that RF transmitters transmit unique identifiers.

B. Federal Communications Commission

The Federal Communications Commission has previously considered requirements for transmittable unique identifiers in several specific scenarios and those examples provide a straightforward blueprint for any potential future rule modifications. In cases where the FCC has adopted rules requiring a service to transmit identifying information, those rules have been adopted as part of the technical rules for the particular service on a case-by-case basis.[2] Should the FCC wish to develop new requirements, it could do so through their regular rulemaking authority.

Furthermore, the FCC's current equipment authorization process, which is already required for RF devices authorized under Part 2 of the Commission's rules, could be used to apply the new requirements

[1] Codified at 47 U.S.C. 902.

[2] Often transmission identifier rules have evolved over time, particularly with the transition from analog to digital transmissions.

to the market.[3] All devices subject to the authorization procedures are required to meet the FCC's technical requirements, which include requirements of no harmful interference emissions.

Today, RF equipment manufacturers already must consult the equipment authorization rules to determine if further technical and administrative rules will apply to a specific product. The technical rules are typically found in the applicable rule parts for the service for which the device will be used. After the device maker has affirmatively determined the applicable rules for the type of device being reviewed, they can then determine what method of authorization applies which is commonly either a Supplier's Declaration of Conformity or Certification. The device must then be submitted to compliance testing and approval upon demonstration of compliance with applicable rules. Finally, the device maker must then meet any applicable labelling, documentation, manufacturing, importation, and/or marketing requirements.[4] Although the administrative process for adding a requirement in the equipment authorization rules to require that all RF transmitters use a unique identifier is straightforward, challenges with the efficacy of such a regime may exist (as discussed further in Section VII below).

IV. Defining a "Unique Identifier"

A 2018 CSMAC Enforcement Subcommittee report explains that " a desirable feature of interference detection is the identification of the interferer or source of interference."[5] One method of identifying the interferer would be to require transmitters to include a unique identifier – assisting in mitigation and accountability. A RF transmittable unique identifier could take a number of forms while providing differing levels of uniqueness, security, privacy, traceability, and utility for interference detection and prevention applications. At its most basic, an identifier useful for interference detection and prevention would likely require at least some identifier data transmission that correlates either a single device or class of devices to an owner or operator that can be contacted to address any interference. Policymakers should consider numerous technical and policy questions when determining the right level of identifier for a specific application, including, for example, likelihood of harmful interference, type of device (e.g., consumer or enterprise), costs (including to the device market and innovation), and security and privacy concerns. Given the significant variation across types and purposes of RF transmitting devices (spanning from garage door openers and walkie talkies to automobiles to complex military defense systems and communications networks) a single uniform protocol across all devices and use cases appears to be infeasible. The sounder approach to addressing specific interference concerns is through use-case tailored identifier requirements.

V. Use of Unique Identifiers

Unique identifiers have been used to identify communications since the early days of wireless communications. For example, call signs or call letters were and are used to uniquely identify transmitting stations. This paper does not attempt to provide a comprehensive guide to every type of

---

[3] *See, e.g.*, Equipment Authorization: Approval Guide, FCC, https://www.fcc.gov/engineering-technology/laboratory-division/general/equipment-authorization.

[4] *Id.*

[5] Report of the Enforcement Subcommittee Commerce Spectrum Management Advisory Committee (CSMAC) July 24, 2018, https://www.ntia.doc.gov/files/ntia/publications/csmac_enforcement_sub-committee_report_072418.pdf.

transmission identifier used by various wireless communications, but provides examples of some common identifiers and examples where agencies have considered whether to implement an identifier.

A. Commercial Applications

1. Unlicensed

Although not a completely unique identifier today, media access control (MAC) addresses are 48-bit unique identifiers deployed to identify the network address in many IEEE 802 networking technologies including Wi-Fi, Ethernet, and Bluetooth, among others. Device manufacturers building devices for these protocols are typically issued a group of identifiers and they then in turn assign specific MAC addresses to individual devices during the manufacturing process, which are stored in read-only hardware or (more commonly today) in software. The preamble of each packet transmitted via Wi-Fi includes the source, destination, and MAC address over an unsecured/open channel.

However, traditional static MAC addresses have been used to log and track nearby devices without users consent or control via targeted probe requests, allowing companies or malicious actors to track an individual's location and movement over time with relative ease.[6] These significant privacy vulnerabilities gave rise to a number of companies developing and implementing techniques to randomize device MAC addresses while unconnected to a network access point in order to address these concerns. However, though a solution to the tracking issue specific, randomizing MAC addresses raises new barriers for network management and optimization as devices are no longer traceable over time. There are also security concerns raised by software-based identifiers which can be used to spoof a device and be leveraged to cause harm to a target of malicious attacks. A recent Liaison Statement to the Wireless Broadband Alliance, the IEEE 802.11 working group "strongly recommends against using any specific MAC address as an identifier for a user or device, outside the scope of the layer 2 communication." However, due to its ubiquity and expected uniqueness, the MAC address continues to be widely used for various purposes, such as security, access control and billing.[7]

The Commission has addressed the concept of unique identifiers in the context of its White Spaces, Unlicensed National Information Infrastructure (U-NII), and 60 GHz rules. The Commission adopted limited use of transmission identifiers in these contexts.

White Spaces. In 2008, in the context of unlicensed fixed TV band devices, the Commission required that all such devices "transmit identifying information and be registered with the database system."[8] The identification signal is required to "conform to a standard established by a recognized industry

---

[6] *See* Lili Herview, MAC Address Randomization: How User Privacy Impacts Wi-Fi And Internet Service Providers, CableLabs (Jul. 28, 2019), https://www.cablelabs.com/mac-address-randomization-how-user-privacy-impacts-wi-fi-and-internet-service-providers, and Status of IEEE 802.11 Randomized and changing MAC address Topic Interest Group, IEEE (last updated Nov. 20, 2019), http://www.ieee802.org/11/Reports/rcmtig_update.htm/.

[7] *Id*.

[8] *Unlicensed Operation in the TV Broadcast Bands; Additional Spectrum for Unlicensed Devices Below 900 MHz and in the 3 GHz Band*, Second Report and Order and Memorandum Opinion and Order, ET Docket No. 04-186, at ¶ 127 (2008) ("*TVWS Repot and Order*").

standards setting organization . . . [and must] carry sufficient information to identify the device and its location.[9] However, at the same time, the FCC did not require personal/portable devises to transmit identifying information when operating, concluding that "an identifying signal will not be of significant value in identifying the source of or, more importantly, resolving any interference that these devices might cause."[10]

U-NII. In 2013, the FCC sought comment on modifications to technical requirements for the U-NII devices that operate in the 5 GHz band.[11] It proposed to require additional device security features and sought comment on whether to "require U-NII devices to transmit identifying information so that, in the event interference to authorized users occurs, [] the source of interference and its location [can be identified]."[12] The FCC also sought comment on what information should be transmitted and in what format. Although at least one commenter supported a transmitter identification requirement, other commenters noted "that current standards do not provide for a convenient way to transmit identifying information, that such information is inadequate to help in resolving harmful interference[.]"[13] Ultimately the FCC declined to require U-NII devices to transmit identifying information, stating that although "a transmitter ID requirement would help to more quickly identify and locate devices that cause harmful interference, we are not persuaded that the benefits accrued from such a requirement would outweigh the costs to implement it at this time."[14]

Additionally, the Commission is recently adopted rules to permit unlicensed operations in the 6 GHz band. The Commission sought comment on whether to require unique identifiers in the 6 GHz band, but the Report and Order concludes that:

> Imposing such a requirement would require us to mandate a modulation format for the transmitted information, which would necessarily impose restrictions on the development of unlicensed technology in the band. Given that the record has provided no details on how this requirement will help resolve interference, we do not believe that imposing this requirement can be justified. We also agree with those commenters who express concern that this requirement could intrude upon the privacy of device users by facilitating tracking of devices.[15]

---

[9] 47 CFR § 15.711(g).

[10] *TVWS Report and Order* at ¶ 128.

[11] *Revision of Part 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (UNII) Devices in the 5 GHz Band*, Notice of Proposed Rule Making, ET Docket No. 13-49, 28 FCC Rcd 1769 (2013).

[12] *Id.* ¶ 51.

[13] *Revision of Part 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (U-NII) Devices in the 5 GHz Band*, First Report and Order, ET Docket No 13-49 at 58 (2014) ("*U-NII Order*").

[14] *Id.* ¶ 60.

[15] *Unlicensed Use of the 6 GHz Band*, Report and Order and Further Notice of Proposed Rulemaking, ET Docket No. 18-295, 35 FCC Rcd 3852, ¶ 228 (2020).

60 GHz. In 2000, when the FCC considered the scope of the transmitter identification requirement in the 60 GHz band, the FCC concluded that indoor equipment would be required to have the ID because it is under the control of the system operator and the operator would be able to decode the ID information to find out which transmitter is interfering with the rest of its system. In contrast, the Commission declined to require the ID for outdoor devices because the victim of interference "would not be able to determine the identity of the manufacturer and thus, the victim could not decode the ID."[16] Subsequently, in 2013, the FCC eliminated the requirement for 60 GHz devices to transmit identification information. Manufacturers noted that eliminating the indoor transmitter ID requirement would lower the costs to develop indoor transceivers.[17] The FCC concluded that "with [] technological advances, co-existence between these 60 GHz devices is better resolved by voluntary standards than by a transmitter identification requirement."[18]

2. Licensed Mobile – 3GPP 4G and 5G protocols

In 1994, the FCC concluded that "CMRS licensees operating on an exclusive basis in Commission-defined service areas should generally be exempt from station identification requirements."[19] Specifically, the FCC exempted nationwide paging licensees and MTA-based SMR licensees from the identification requirements because "such licensees can readily be identified based on service area information contained in the Commission's licensing records and other publicly available sources."[20] The FCC permits licensees that are still required to transmit station identification to do so digitally, so long as the licensee provided the FCC with information sufficient to decode the transmission. However, licenses on shared channels may not transmit their call signs digitally because "licensees who experience interference on a shared channel indicate that they would not be able to identify the source of such interference based on a digital call sign transmission."[21]

Although the FCC chose not to require a unique identifier for interference purposes, industry developed cellular protocols do include an International Mobile Equipment Identity (IMEI) in order for the network to identify valid devices that can connect. Since the IMEI is often unique (although not always) and transmitted with each RF transmissions it provides another example of an existing identifier that could

---

[16] *Revision of Part 15 of the Commission's Rules Regarding Operation in the 57-64 GHz Band*, Report and Order, ET Docket No. 07-113, RM-111-4, FCC 13-112 ¶ 41 (Aug. 9, 2013).

[17] *Id.* ¶ 42.

[18] *Id.* ¶ 43.

[19] *Implementation of Sections 3(n) and 332 of the Communications Act; Regulatory Treatment of Mobile Services Amendment of Part 90 of the Commission's Rules To Facilitate Future Development of SMR Systems in the 800 MHz Frequency Band Amendment of Parts 2 and 90 of the Commission's Rules To Provide for the Use of 200 Channels Outside the Designated Filing Areas in the 896-901 MHz and 935-940 MHz Band Allotted to the Specialized Mobile Radio Pool*, Third Report And Order, 9 FCC Rcd 7988, 8092, ¶ 216 (1994) ("*Part 90 Third Report and Order*").

[20] *Id.* Today the rule exempts "929-930 MHz nationwide paging licensees or MTA or EA-based SMR licensees." 47 CFR 90.425(e).

[21] *Id.* at 8093 ¶ 219.

be considered for any potential interference detection frameworks involving cellular or related devices and protocols. A short overview of identifiers used on cellular networks is provided below.

Cellular network technologies have evolved over several generations, including 2G, 3G, and 4G, and 3GPP (3rd Generation Partnership Project) is actively developing 5G specifications which include a unique identifier transmitted with each RF transmission.[22] Historically, existing protocols in mobile networking have been vulnerable to several significant security concerns because of their identification techniques, throughout previous and current generations, including:

- *Lack of network authentication in 2G (first launched in 1991), resulting in attacks such as network spoofing by faked base stations*—For example, a faked base station can advertise a different tracking area code with a stronger signal strength to lure user equipment (UE) away from its legitimate cellular network to register with the faked base station. As a result, the faked base station can then send text messages to the UE and thus attempt to defraud the user.

- *Lack of integrity protection for certain signaling messages, thus allowing signal spoofing and tampering*— For example, an Identity Request (a non-access stratum [NAS] signaling message in Long-Term Evolution [LTE]), if not protected with authentication and integrity, can be sent by a faked base station to steal UE permanent identifiers, e.g., the international mobile subscriber identity (IMSI).

- *Lack of confidentiality in certain signaling messages, resulting in privacy violation*—For example, paging information, which is not encrypted, can be used to detect the presence of a particular user and even to track the user to a precise location.[23]

In order to help address and mitigate these issues going forward, the 3GPP defines an Authentication and Key Agreement (AKA) protocol and procedures that support entity authentication, message integrity, and message confidentiality, among other security properties. The 3GPP AKA protocol is a challenge-and-response authentication protocol based on a symmetric key shared between a subscriber and a home network. After the mutual authentication between a subscriber and a home network, cryptographic keying materials are derived to protect subsequent communication between a subscriber and a serving network, including both signaling messages and user plane data (e.g., over radio channels).[24] A unified authentication framework has been defined to make 5G authentication both open (e.g., with the support of Extensible Authentication Protocol [EAP], the device authentication procedure allows devices to move between adjacent networks such as Wi-Fi or cable without reauthentication) and access-network agnostic (e.g., supporting both 3GGP access networks and non-3GPP access networks

---

[22] A Comparative Introduction to 4G and 5G Authentication, CableLabs (Winter 2019), https://go.cablelabs.com/hubfs/InformED%20Insights/A%20Comparative%20Introduction%20of%204G%20and%205G%20Authentication.pdf?__hstc=217413636.9422873fff8c7247165d865f9698b8fc.1581621282610.1581621282610.1582044580604.2&__hssc=217413636.1.1582044580604&__hsfp=4225248186.

[23] *Id.*

[24] *Id.*

such as Wi-Fi and cable networks).[25] 5G protocols also send a Radio Network Temporary Identifier (RNTI), which via the operator could be linked to the permanent IMEI and a specific device. These RNTI numbers are transmitted with each transmission and could provide a potential method for tracing interference through a mobile network operator if needed.

3. Citizens Broadband Radio Service

The Citizens Broadband Radio Service (CBRS) provides an example where a band-specific interference protection mechanism is being deployed. The three-tiered sharing framework incorporates a dynamic spectrum database and interference mitigation techniques to manage three tiers of users (incumbent users, Priority Access Licensees, and General Authorized Access users).[26] In response to these requirements, the WinnForum's deployment guidelines require using a central managed authority and unique identifiers (e.g. Public Key Infrastructure) for CBRS users.[27] CBRS uses the centralized spectrum access system (SAS) and environmental sensing capability (ESC) network to determine when an incumbent federal user is using a frequency in order to dynamically shift CBRS user traffic to other channels or frequencies.

4. Upper Microwave Flexible Use Service (UMFUS)

The FCC considered and rejected to notion of unique identifiers for interference mitigation purposes in higher frequency bands for a number of reasons, including the inherent propagation limitations of higher frequencies. In 2017, the FCC declined to require mmWave band licensees (28 GHz, 39 GHz, 37 GHz and 64-71 GHz) to transmit digital identifiers. The FCC explained that " the record provides insufficient support for the adoption of digital ID requirements for these mmWave bands, particularly if we were to specify a particular format. . . . [C]haracteristics of the mmWave bands at issue [] make the occurrence of interference less likely in the first instance, relative to other bands. . . . [and] technologies being developed specifically for these bands should also make it easier for operations to co-exist in the same vicinity without causing interference to one another. We acknowledge the important role of the agency in identifying and locating devices that cause harmful interference, but we find that it is unnecessary and unsupported in the case of these mmWave bands to adopt a digital ID requirement."[28]

5. Private Land Mobile Radio Services (PLMR)

Stations licensed under Part 90 have long been required to transmit identification information in the form of the assigned call sign – generally by voice or Morse code.[29] However, in 2013, the FCC modified

---

[25] *Id.*

[26] *Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550- 3650 MHz Band*, Report and Order and Further Notice of Proposed Rulemaking, GN Docket No. 12-354 (2015).

[27] Approved CBRS Root CA Operators, CBRS WInnForum Standards, https://cbrs.wirelessinnovation.org/cbrs-root-ca-operators.

[28] *Use of Spectrum Bands Above 24 GHz for Mobile Radio Servs.*, Second Report and Order, 32 FCC Rcd 10988, 11066 ¶¶ 271-72 (2017) ("*UMFUS Report and Order*").

[29] 47 CFR § 90.425.

its rules to permit PLMR stations with exclusive channels to transmit their call signs digitally.[30] The FCC noted that "some commenters asked that digital transmission of [] station identification be readable without specialized equipment."[31] The FCC chose to make digital transmission of the station identification voluntary so long as a station provides the FCC with information to decode the digital transmission, stating: "by limiting this option to exclusive-use licensees, we do not anticipate that this will cause any significant increase in interference complaints or result in any significant impairment of the ability of licensees to work with each other in resolving interference problems. Therefore, we find that the benefits of granting flexibility with respect to call sign transmission outweigh any associated costs."[32]

6. Broadband Video Uplinks

Section 25.281 of the Commission's rules requires broadband video uplinks to include a subcarrier signal identifying the transmitting earth station's call sign and including contact information. That identification signal is called an "automatic transmitter identification system" (ATIS)[33] and was intended to "facilitate rapid identification of sources of interference and prompt resolution of interference problems." In 1986, the FCC sought comment on requiring an ATIS.[34] Many of the comments at that time focused on deficiencies of the rigidly proposed system because it was incompatible with certain specific systems, it increased channel occupancy, or it was economically unsound. The FCC adopted ATIS rules for broadband video satellite uplink signals in 1990.[35] Subsequently, in 2013, the FCC modified the ATIS rules to account for new digitally modulated broadband video signals.[36] Among other things, the FCC modified the scope of the rules to apply only to analog video transmissions and digitally-modulated video uplinks from SNG vehicles and other temporary-fixed earth stations, noting that other transmissions did not appear to be a significant source of interference and that there was a lack of industry consensus on how to implement an ATIS technique for "burst" transmissions.[37] The FCC decided that the rules should "incorporate by reference the industry standard for carrier ID rather than

---

[30] Amendment of Part 90 of the Commission's Rules, 28 FCC Rcd 5924, 5924 (2013) ("*Amendment to Part 90*"); see also 47 CFR § 90.425(c).

[31] *Amendment to Part 90* at 5930 ¶ 15.

[32] *Id*. at 5931 ¶ 16.

[33] The FCC described the ATIS as "a unique, unchangeable identifying number assigned to each transmitter at time of manufacture plus some correlation of the number to a data base identifying the licensee, such as a call letter list." The "information is automatically modulated onto the unit's transmission, [and becomes a] 'signature; providing positive identification of each radiated signal." *An Automatic Transmitter Identification System for Radio Transmitting Equipment*, Notice of Proposed Rule Making and Notice of Inquiry, FCC 86-358 (1986) ("ATIS NPRM").

[34] *Id.* ¶ 8.

[35] *An Automatic Transmitter Identification System for Radio Transmitting Equipment*, Report and Order, 5 FCC Rcd 3256 (1990).

[36] *Comprehensive Review of Licensing & Operating Rules for Satellite Servs.*, FCC 13-111, ¶ 206 (2013) ("*ATIS Report and Order*").

[37] *Id.* ¶ 210.

specifying detailed technical characteristics of the spread spectrum carrier ID method."[38] The FCC required that the ATIS message continuously repeat and that "ATIS equipment must be integrated into the uplink transmitter chain with a method that cannot easily be defeated."[39]

7. Federal Aviation Administration's UAS Remote Identification Proposal

The Federal Aviation Administration recently published a Notice of Proposed Rulemaking (NPRM) on a set of new rules applying to drones and other unmanned aircraft systems (UAS) to address rising safety and security concerns with these devices operating alongside traditional airspace users.[40] The proposal centers around requiring drones and UASs to register individually and broadcast an identifier in order to operate in most locations. The proposed rules seek to "tie the remote identification requirements to the registration of unmanned aircraft because the FAA and law enforcement agencies have a need to correlate remote identification and registration data." The rules would require a unique identifier such as the serial number be broadcast while the UAS is flying via wireless internet connectivity.

The proposed required message elements include, among others, a UAS Identification to establish the unique identity of the UAS. Operators would have to choose whether to use the serial number of the unmanned aircraft or a session ID (*e.g.,* a randomly generated alphanumeric code assigned by a Remote ID USS on a per-flight basis designed to provide additional privacy to the operator) as the UAS Identification.[41]

In situations where the UAS does not have connectivity itself, the FAA proposes that the controller might supply and broadcast the identifier. In situations where neither the UAS nor the controller are able to connect, the device itself would need "a functioning broadcast capability is necessary in order for remote identification information to be available in areas that do not have wireless internet connectivity."[42] Comments were due on this proposed rulemaking on March 2, 2020.

B. Government Applications

The NTIA "Manual of Regulations and Procedures for Federal Radio Frequency Management (Redbook)," is incorporated by reference in the federal code in 47 CFR § 300.[43] The Redbook sets forth various requirements for Federal equipment and its use of radio frequency spectrum. The NTIA Redbook requires the use and transmission of unique identifiers in the context of call signs, providing recommended practices across several applications. For example, for fixed and land based radio operations, the Redbook states that "[e]ach station shall transmit its assigned call sign on each

---

[38] *Id*. ¶ 213.

[39] 47 CFR § 25.281.

[40] UAS Remote Identification, Dkt. No. FAA-2019-1100, 84 FR 72438 (Dec. 31, 2019), https://www.federalregister.gov/documents/2019/12/31/2019-28100/remote-identification-of-unmanned-aircraft-systems.

[41] *Id*. at 72465.

[42] *Id*.

[43] 47 CFR § 300.1.

frequency in use at the beginning and end of operation, and at least once an hour. More frequent identification may be made if delay to traffic will not result."[44] In mobile applications, devices are not required to transmit any identification if they "transmit[] only on the transmitting frequency of the associated base station." If the mobile device transmits "on any frequency other than the transmitting frequency of the associated base station, or which has no associated base station, shall transmit the required identification at the end of each transmission or exchange of transmission or once each hour of the operating period." In such cases the identification requirements are the same as for fixed services unless subject to another applicable provision (e.g. maritime mobile service is subject to the applicable provisions of the ITU Radio Regulations and all other international agreements in force to which the United States is a party).[45] The Redbook specifically exempts RF devices that "are entirely automatic in their operation such as telemetering, hydrological and weather reporting, and aeronautical instrumentation…"[46]

Although there certainly may be additional examples where the federal government has successfully required transmittable unique identifiers in RF device deployments, the practice does not appear to be widespread or commonly used.

VI. Assessing the Benefits of Unique Identifiers

The Subcommittee's agrees with its tentative conclusion that the use of unique transmission identifiers is likely to always be helpful in the context of interference detection and resolution, but a requirement that emitters transmit unique identifiers (whether specific to a device or a class of devices) does not come without cost or challenges. Therefore, policymakers should weigh technological capabilities, costs, and benefits when deciding whether to require the use of a transmit identifier.

The FCC's decisions point to several considerations that have guided when the unique identifiers have been required by the agency.

- Where licenses operate on shared channels, the FCC is more likely to require transmission identifiers and to ensure that licensees who experience interference will be able to identify the source of interference (i.e., not permitting digital transmissions where those receiving interference would be unable to use the digital call sign transmission to identify the source of interference).

- Where interference would occur to critical/government users, the FCC has taken steps to require unique identifiers that can be used in interference detection and resolution.[47]

---

[44] Manual of Regulations and Procedures for Federal Radio Frequency Management, NTIA, U.S. Dept. of Comm. (Sept. 2017 Revision of the May 2013 Edition), available at https://www.ntia.doc.gov/files/ntia/publications/ntia_manual_september_2017_revision.pdf.

[45] *Id*.

[46] *Id*.

[47] *See, e.g.*, *3.5 GHz Report and Order*.

- Where licensees can readily be identified based on service area information contained in the Commission records or other publicly available sources, the FCC has declined to impose transmission identifier requirements.[48]

- Where the FCC does not believe an identification signal will be of significant value in identifying the source of or resolving interference that devices may cause (e.g., requiring personal/portable devices to transmit identifying information when operating, may not be helpful because such devices move around), it has declined to require transmission identifiers.[49]

- Where industry standards do not exist or do not seem likely to develop, the FCC has declined to impose transmission identifiers.[50]

- Where a rule requiring the transmission of unique identifiers is likely to restrict the development of a technology or ecosystem, the FCC has expressed reluctance to mandate use of a such an identifier.[51]

- Where the characteristics spectrum make the occurrence of interference less likely, relative to other bands, the FCC has declined to require transmission identifiers.[52]

To aid its evaluation unique identifiers and further explore when that tool would be most useful and practical to implement in the real world, the Subcommittee discussed NTIA's question with a number of industry experts with direct experience in the evaluation, tracing and remediation of interference complaints: Rhett Butler, Project Manager at Comsearch;[53] Paul Denisowski, Project Engineer at Rohde & Schwarz;[54] Jay M. Jacobsmeyer, P.E, Owner of Pericle Communications Company;[55] and Milo Medin, Vice President of Access Services at Google, Inc.[56]

The Subcommittee asked the experts whether unique transmit identifiers would be helpful in identifying and resolving cases of harmful interference. As a general matter, the experts agreed that unique transmit identifiers are helpful tools, but they questioned the practicality of requiring unique identifiers for all emitters.

Mr. Medin explained that, at the highest level, there is a spectrum of possible identifiers from a simple callsign (which is not authenticated) all the way up to a digitally and encrypted hardcoded identifier (e.g.

---

[48] *See, e.g.*, *Part 90 Third Report and Order*.

[49] *See, e.g.*, *TVWS Report and Order*.

[50] *See, e.g.*, *U-NII Order*; *ATIS Report and Order*; *UMFUS Report and Order.*

[51] *See, e.g.*, *U-NII Order*.

[52] *See, e.g.*, *UMFUS Report and Order*.

[53] https://www.linkedin.com/in/rhett-butler-53a58057/

[54] https://www.rohde-schwarz.com/us/solutions/test-and-measurement/mobile-network-testing/interference-hunting/ihuntertraining-webinars_250575.html

[55] https://www.pericle.com/company/our-people/

[56] https://innovation.defense.gov/Media/Biographies/Bio-Display/Article/1395855/milo-medin/

MAC protocol or frame structure) existing today. Furthermore, that while device identifiers, such as an IMEIs, are widely used today in cellular technologies, they are not necessarily unique and can be spoofed and copied by malicious actors. However, these identifiers are improving and continue to get better cryptographic and security capabilities with each new generation of protocol.

Mr. Jacobsmeyer indicated that unique transmission identifiers would always be helpful in theory, but may not always be a practical, especially for services that already have equipment deployed. Mr. Denisowski, had a similar perspective, suggesting that if through a unique identifier he could determine who owned a device, or where it was physically located (within meters), that identifier would solve the vast majority of interference cases. However, he noted that the practical implementation of such a system would be problematic on a wide-scale, particularly if one attempted to modify existing devices to incorporate unique transmit identifiers.

The experts noted that unique identifiers may not help in all circumstances. For example, Mr. Butler and Mr. Denisowski both indicated that more than half the cases of interference come from unintentional radiators (such as air conditioning units, streetlights, microwave ovens, etc.) that are emitting unmodulated signals, and in such cases, a transmitted unique identifier could not be used to expedite interference location process. Mr. Denisowski emphasized that there are many cases of interference caused by spurious sources of RF that have no capability to transmit an identifier. Mr. Butler also noted that aggregate interference is challenging to resolve, and unique identifiers may not address that problem. Finally, all of the experts noted that even where there are unique identifiers there will still be cases where deliberate jammers work to circumvent the identifier.

Speaking on the utility of a transmit identifier, Mr. Denisowski noted that a unique identifier is only helpful to the extent the person receiving interference can demodulate the ID. For example, with paging systems, the identification is done in Morse Code and can be looked up in an FCC database. Without the ability to tie an identifier back to a device or device owner the unique identifier will not be as much help in quickly resolving interference. The Subcommittee discussed this topic with Mr. Butler as well, and he noted that where information ties back into a database, the information is only as good as it is accurate. He pointed to examples where systems are sold and resold, but the FCC's database still has the original owner's records. Mr. Denisowski indicated that in his experience, even in cases where the source of interference could be identified (either spectrally or through demodulation of the signal), direction finding is still required.

The Subcommittee asked the experts whether having an identifier for a class of devices would be helpful in lieu of an identifier that was specific to a device's location or owner. Mr. Jacobsmeyer, Mr. Butler, and Mr. Denisowski all said that a broad identifier such as the class of devices would be a helpful datapoint, but they did not know how much that information could truly speed up the interference hunting process. For example, Mr. Butler suggested that while a class of unique identifiers might be occasionally helpful in mobile interference cases, most of the interference issues involve a static interferer with known entities in a licensed band which diminishes the potential value of a class-based identifier. He noted that he frequently sees interference situations where there are a number of operators with equipment at a single location (e.g. a rooftop) and even though the location is known, determining which equipment and operator's equipment is causing the issue is difficult. He often sees this scenario arise where WISP operators that have mistakenly tuned their network equipment beyond the appropriate frequencies and begin causing interference to adjacent systems (e.g. operators on the C-band). Mr. Medin suspected that while using broad classes of identifiers that identify the device type only would be useful in finding an interference source, while resolving some privacy and security

concerns, there are still common interference contexts where the application would be complex and not necessarily succeed in helping mitigate the interference. One such example is where interference is generated by the solar edge inverters commonly used in residential solar power generation installations. Since the device is unintentionally radiating interference rather than attempting to transmit, while an identifier that provided the device type could be valuable (e.g. knowing the interference is a solar edge optimizer) if it can be decoded from the interference. However, requiring manufacturers to add beacons in microinverters would not help find most cases of interference because the device is not attempting to transmit (where a identifier could be decoded) but rather radiating interference pollution unintentionally. While a device type identifier might not be valuable for passive interference from solar inverters, Mr. Medin suggested that using an existing device type identifier such as the Organizationally Unique Identifier (OUI) used in some unlicensed transmission systems such as Bluetooth and Wi-Fi, could strike an appropriate balance between preserving privacy while providing a helpful way to track interference in those systems.

Mr. Butler also noted the potential competitive concerns around the issue of who has the authorization and ability to decode an identifier. He agreed that interference hunters would benefit from access to identifier data, but concerns exist around revealing competitive intelligence and corporate secrets, device configuration, and the geography of companies' networks. Mr. Denisowski observed that unique identifiers could be a security issue in or near sensitive facilities (e.g. do we want someone to be able to drive around the White House and create a map of all the wireless devices, including type, owner, and location). It could also be an issue for agencies involved in (counter)surveillance that do not want to broadcast their presence.

Finally, Mr. Jacobsmeyer, Mr. Medin, Mr. Denisowski, and Mr. Butler all noted that as a general rule, it is easier to build requirements for unique transmit identifiers into new bands and services than to retroactively require devices to begin transmitting unique identifiers. All of the experts agreed that it would be complicated and costly to retrofit existing devices to broadcast a unique identifier. But even in new devices and services, Mr. Butler pointed out that cost and energy burn are a potential barrier to the use of unique identifiers. New entrants want to be cost effective, and particularly with Internet of Things devices, equipment manufacturers are worried about the size of a device and its battery life. Mr. Denisolwski agreed the cost of implementing unique identifiers would most likely be considerably higher if the ID were transmitted "out of band" (i.e. not on the same frequencies the device "normally" transmits on). Having a second transmitter would increase cost and complexity, and require additional design, testing, and debug to be sure that the "primary transmitter" and "ID transmitter" don't interfere with each other.

Mr. Medin underscored that difficulties in repurposing or creating a new unique identifier for interference detection and mitigation purposes arise in the transmission, modulation and decoding of the identifiers. He noted that creating a protocol for the transmission, modulation and decoding of a unique identifier will be more feasible in the context of new ground up communications systems (e.g. CBRS) rather than existing ecosystems (e.g. Wi-Fi). Mr. Jacobsmeyer and Mr. Medin both discussed how the CBRS framework is an example of a regulatory and technological model that largely addresses many interference concerns (although the CBRS band has not been fully tested in the real world yet). Mr. Medin suggested that the digital prefix used in the CBRS protocol might provide an example of where adding device location data in the header identifier could help locate rogue operators. He also noted that although malicious intentional interferers (e.g. circumventing authentication checks via code) will always be a problem, but, with the active registration and certification requirements in the equipment

that require cryptographic authorization in the CBRS band, much bad interference behavior can be disincentivized and removed.

Based on FCC precedent and the Subcommittee's discussions with interference experts, the subcommittee notes that three gating questions could assist policymakers in deciding which bands or services are good candidates to explore the use of unique identifiers are: (1) how often will/does harmful interference occur; (2) how consequential would the harmful interference be to affected users, and (3) how difficult will it be to identify and remedy the cause of the interference. The more often or consequential the interference is, and the harder it is to remediate with other tools (for example, database registration where devices are fixed), the stronger the case for at least exploring whether to require devices to transmit unique identifiers to facilitate interference detection and resolution. It should be noted that policymakers may consider beneficial applications of unique identifiers outside of interference detection and resolution context. For example, some have suggested using RFID as a unique identifier solution to the difficulties in vehicle identification and authentication.[57]

VII. Challenges to Requiring the Transmission of Unique Identifiers

Below we discuss some of the challenges and costs associated with requiring the transmission of unique identifiers in devices, these factors inform the discussion about each band's operating environment – set out above.

A. Standards Development and Technology Changes

Given the vast number of technologies, many proprietary, mandating the transmission of unique identifiers creates significant challenges. For this reason, the FCC has often looked to standards bodies to play a role in designing protocols for the transmission of unique identifiers (for example in the ATIS context, or with CBRS). However, standards can take years to evolve and technology can change rapidly necessitating continued evaluation of standards and protocols. In the context of the ATIS, the FCC acknowledged that "no single code scheme will function in all situations."[58]

B. Device Capabilities

To the extent that policymakers decide to utilize transmit IDs in services that already exist and have equipment that is already deployed, backward compatibility would have to be examined, unique to each type of equipment. Rarely is equipment rolled out at one time, and some equipment has a multi-decade lifecycle (for example, public safety equipment).

---

[57] A recent research paper suggested that using RFID as a global identifier would be a better approach than a user ID for security frameworks to authenticate vehicles and keep track of their information. The paper notes that "a global ID focuses on a hardcoded identification number given to each vehicle during manufacturing and stored in an RFID tag. This RFID can be used for vehicle identification . . . and can also help with issues such as accountability in accidents. The global ID can also help minimize impersonation attacks and false information distribution, and aid in catching malicious devices falsifying registration or environmental data." *See* A. Nanda, D. Puthal, J. J. P. C. Rodrigues and S. A. Kozlov, "Internet of Autonomous Vehicles Communications Security: Overview, Issues, and Directions," in *IEEE Wireless Communications*, vol. 26, no. 4, pp. 60-65, August 2019, doi: 10.1109/MWC.2019.1800503.

[58] *ATIS NPRM* ¶ 8.

Additionally, some equipment would need to be modified or designed to transmit a unique identifier. Equipment that relies on battery power may be significantly impacted by unique identifier requirements because the transmission of a unique identifier will strain battery power (the impacts are likely to vary from minor to significant). As a general guideline, the addition of a unique identifier will put increasing pressure on battery manufacturers to increase size and capability of batteries, with attendant increase in device size and cost.

One example from the Subcommittee's conversations with Mr. Jacobsmeyer and Mr. Denisowski illustrates the limitations using a unique transmission ID will all types of devices. Mr. Jacobsmeyer and Mr. Denisowski both found that one of the most frequent case of interference they are called on to help with today, and a prevalent source of interference throughout the nation, comes from improperly installed Bi-Directional Amplifiers (BDAs). These devices are essentially two-way radio communications signal boosters used to ensure public safety in buildings during times of emergency. Almost every city or county in the United States has mandatory codes and ordinances to guarantee a minimum level of communications system reliability for first responders.[59] Although the existence of a unique identifier could be helpful in locating the exact BDA causing an interference problem, the technology used in these devices may not be conducive to the use of transmitted IDs. The device itself does not transmit; it repeats a transmission. Therefore, to transmit a unique identifier, BDAs would need to be reconfigured or redesigned to have some sort of independent transmission capability. Additionally, a transmission by the BDA would have to share spectrum in time with the desired retransmission, which in itself could cause interference to occur – making the solution as harmful as the problem.

C. Privacy and Security Concerns

Regardless of how broadly an identifier requirement is applied, a key dimension to consider is the identifier's security. As evidenced by the recent rise in insecure IoT devices being leveraged for nefarious botnets,[60] the consequences of weak security in numerous, small devices can be compounded into a significant threat. While not alone sufficient to solving botnets, a secure identifier is a key requirement for many solutions. A short discussion of some of the key requirements of a secure unique identifiers follows.

While a uniform technical protocol for a RF based transmittable and globally unique identifier does not exist today, such a uniform could take a number of forms with differing levels of technical complexity, security levels, and privacy risks associated with each. Not all unique device identifiers are equal. In order to support strong security, the device identifier must be immutable, attestable, and unique. Today, for example, IoT devices typically do not use identifiers that are both unique and immutable and the device identifiers are almost never attestable. Attestability enables the device identity to be cryptographically verified, dramatically reducing the risk that the device is being impersonated (or "spoofed"). A strong unique device identifier (i.e., immutable, attestable, and unique) is the necessary

---

[59] *See, e.g.*, DC Government's Office of Unified Communications, OUC's Public Safety In-building Radio Systems Requirements, https://ouc.dc.gov/page/oucs-public-safety-building-radio-systems-requirements.

[60] *See e.g.*, A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats, Dept. of Comm. & Dept. of Homeland Security (May 22, 2018), https://csrc.nist.gov/CSRC/media/Publications/white-paper/2018/05/30/enhancing-resilience-against-botnets--report-to-the-president/final/documents/eo_13800_botnet_report_-_finalv2.pdf.

foundation to ensuring any potential identifier-based interference detection and protection framework is secured and malicious actors cannot easily leverage the framework for harmful use.

While technology exists to provide strong device identity, it has yet to be widely adopted by RF device makers outside of certain industries and use cases. For example, the cable industry has long incorporated strong device identity in its cable modems, set-top boxes, and other devices directly connected to the cable network, using a public key infrastructure (PKI). Critically, certificate management is the mechanism that enables attestation, which not only enables verification, but also revocation – allowing the certificate manager to deprecate or completely revoke a certificate and communicate that revocation in response to future inquiries. In turn, certificate management enables enforcement of security standards among and between devices, as discussed in more detail below. The certificate manager can serve as the authoritative source as to whether a device has passed the certification test associated with the security standard. For example, to protect itself, a connected healthcare device might only communicate with other devices that have been certified to meet a higher level of security within the standard. The healthcare device can query with the certificate manager (or certification authority), using the digital certificate of the other device, to verify whether that device actually complies with the necessary security standards.

Certificate management and the ability to revoke certificates also provides an automated mechanism to ensure ongoing compliance with a security standard or to communicate compromises or known vulnerabilities for devices. For example, if a device initially passes certification testing, but a critical security vulnerability is discovered or the manufacture then makes changes (e.g., adds additional features) that cause the device to no longer comply with the security standard, the certificate manager can revoke those certificates until the manufacturer addresses the issue. More generally, with a certificate manager, anyone (the ISP, another device, or smart home hub) can query whether a device is and remains compliant with the security standard and if not, deprecate that device's privileges.[61] Furthermore, a secure unique identifier should include a mechanism to limit responses to untrusted requests from (e.g., anonymous) devices. Providing a device's unique and immutable identifier to any and all requests creates security risk. For example, a mobile device, such as a Bluetooth fitness band, that broadcasts its unique and immutable identifier whenever requested, enables easy tracking of the device and its owner without the owner's knowledge or consent.[62] To the extent unique identifiers rely on a certificate system, or some other system that must be administered, questions arise as to who administers the program, the cost of certificates, how they are distributed to devices, and what happens if the root is compromised.

Unique transmit IDs associated with unlicensed consumer devices carry particular privacy concerns. Consumer devices are often carried throughout the course of their day. Unique identifiers transmitted from those devices could be collected from access points and could be easily associated with a specific consumer's location. Questions arise around who has access to that information, how it is stored, and

---

[61] A Vison for Secure IoT, CableLabs (Summer 2017), https://www.cablelabs.com/insights/vision-secure-iot/.

[62] *See, e.g.*, Andrew Hilts, "Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security," Open Effect (Feb. 2, 2016), https://openeffect.ca/fitness-tracker-privacy-and-security/ ("Seven out of eight fitness tracking devices emit persistent unique identifiers (Bluetooth Media Access Control address) that can expose their wearers to long-term tracking of their location when the device is not paired, and connected to, a mobile device.").

whether consumers have any control over those questions. As discussed in Section V.A.1 above, MACs which identify RLANs, were randomized due to privacy concerns. But even with the generation of random MAC addresses, privacy issues continue to be raised.[63]

The active transmission of unique identifiers would likely have implications for national security as well. For example, stealth technology is created to minimize detection. A requirement that all emitting devices transmit a unique identifier could run contrary to the goal of such technology. Likewise, the military has recently restricted the use of consumer devices where applications capture data that puts bases at risk.[64] To the extent all RF equipment, including military equipment, were required to transmit a unique identifier, questions about protecting who has access to that data and how to protect it would certainly arise in the context of national security.

D. Impact on Investment and Innovation

A further consideration in any transmittable unique identifiers discussion is the risk that such a requirement will increase equipment costs, stymie innovation, and create new barriers to entry. Onerous technical and compliance requirements mandating unique identifiers could particularly discourage investment and innovation in newly cleared frequencies by increasing costs and uncertainty for new entrants looking to develop compatible technologies. The Organisation for Economic Co-operation and Development has explicitly recognized this tradeoff as an inherent consideration to regulatory reform, and many others have observed the effect enhanced in technology markets where certain conditions such as high uncertainty are often observed. In such cases, research suggests "formal standards generate lower compliance and consequently innovation costs as they provide a better fit to the existing technological opportunities, while regulations have the opposite effect."[65]

The technical development, manufacturing, and energy costs of adding secure identifiers and transmission capabilities to all devices are likely to be significant. This risk seems particularly apparent for the innovative applications of low power IoT devices. The broad risk of dampening technology innovation and investment is inherently present and should be carefully weighed against any perceived specific benefits of new rules.

---

[63] *See, e.g.*, TechCrunch, *London's Tube network to switch on Wi-Fi tracking by default in July* (May 22, 2019), https://techcrunch.com/2019/05/22/mind-the-privacy-gap/ (providing an example of the privacy concerns about the use of random MAC addresses).

[64] *See, e.g.*, AP, *Pentagon restricts use of fitness trackers, other devices* (Aug. 6, 2018), https://apnews.com/d29c724e1d72460fbf7c2e999992d258/Pentagon-restricts-use-of-fitness-trackers,-other-devices.

[65] *See, e.g.*, Tim Day, When It Comes to Tech, It's Regulation vs. Innovation, U.S. Chamber of Commerce (Aug. 18, 2017), https://www.uschamber.com/series/above-the-fold/when-it-comes-tech-it-s-regulation-vs-innovation; Knut Blind, Sören S. Peterson, & Cesare A.F. Riilo, The Impact of Standards and Regulation on Innovation in Uncertain Markets, Research Policy Vol. 46, Issue 1 (Feb. 2017), https://doi.org/10.1016/j.respol.2016.11.003.