Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Wireless E911 Location Accuracy Requirements	)	PS Docket No. 07-114
	)	

MEMORANDUM OPINION AND ORDER

Adopted: November 13, 2017 **Released: November 14, 2017**

By the Commission:

I. INTRODUCTION

1. In this *Memorandum Opinion and Order*, we approve the Privacy and Security Plan (Plan) for the National Emergency Address Database (NEAD) submitted on February 3, 2017, by national wireless carriers AT&T, Sprint Corporation, T-Mobile USA, and Verizon (collectively, National Carriers) and NEAD, LLC.[1] The NEAD, which is being developed for the purpose of identifying the dispatchable location of wireless 911 callers when the caller is indoors,[2] is a database that will enable wireless providers to use media access control (MAC) address and Bluetooth Public Device Addresses (BT-PDA) information of fixed indoor access points to locate wireless devices being used to call 911.[3] For the reasons discussed below, we approve the Plan, finding that it is consistent with the requirements outlined in the *Indoor Location Fourth Report and Order* and addresses the need to protect the privacy, security, and resiliency of the NEAD.

II. BACKGROUND

2. In the *Indoor Location Fourth Report and Order*, the Commission adopted E911 location rules that encourage the development of wireless E911 location technology that will support the provision of dispatchable location information (e.g., street address, floor level, and office or apartment number) to Public Safety Answering Points (PSAPs) when wireless customers place 911 calls from indoor locations.

[1] *See* NEAD, LLC, AT&T, T-Mobile USA, Sprint Corporation, and Verizon, NEAD Privacy and Security Plan, PS Docket No. 07-114 (Feb. 3, 2017) at https://ecfsapi.fcc.gov/file/1020387572432/170203%20NEAD%20Privacy%20and%20Security%20Plan.pdf (Plan); *see also* Letter from NEAD, LLC, AT&T, T-Mobile USA, Sprint Corporation, and Verizon, to Marlene H. Dortch, Secretary, Federal Communications Commission, (Feb. 3, 2017) (on file in PS Docket No. 07-114, at https://ecfsapi.fcc.gov/file/1020387572432/170203%20Cover%20Letter%20to%20NEAD%20Privacy%20and%20Security%20Plan.pdf) (Cover Letter).

[2] *See Wireless E911 Location Accuracy Requirements*, Fourth Report and Order, 30 FCC Rcd 1259 (2015) (*Indoor Location Fourth Report and Order*) and rules at 47 CFR § 20.18(i) *et seq*.

[3] *See* 47 CFR § 20.18(i)(1)(iii); *Indoor Location Fourth Report and Order*, 30 FCC Rcd at 1279, para. 55. "Dispatchable location" is "a location delivered to the PSAP by the CMRS provider with a 911 call that consists of the street address of the calling party, plus additional information such as suite, apartment or similar information necessary to adequately identify the location of the calling party. The street address of the calling party must be validated and, to the extent possible, corroborated against other location information prior to delivery of dispatchable location information by the CMRS provider to the PSAP." 47 CFR § 20.18(i)(1)(i); *see also Indoor Location Fourth Report and Order*, 30 FCC Rcd at 1273-74, paras. 43-44.

To support dispatchable location, the National Carriers have committed to design and build the NEAD, a national database of MAC address and BT-PDA information of fixed indoor access points (e.g., Wi-Fi and Bluetooth) that will be used to determine the specific indoor location of wireless 911 callers and play a critical role in enabling carriers to satisfy the Commission's E911 rules.

3. The *Indoor Location Fourth Report and Order* required the NEAD to be used solely for 911 location purposes and prohibited its use for commercial purposes.[4] The Commission also stated that as a precondition of activating the NEAD, the four nationwide carriers must develop a privacy and security plan for the NEAD and submit it for Commission approval.[5] Further, the Commission stated that it would make the submitted plan available for public comment to "ensure that [it] addresses the full range of security and privacy concerns that must be resolved prior to use of the database."[6] The Commission stated that upon review of the plan and the record generated in response, it would "evaluate the need to take any additional measures to protect the privacy, security, and resiliency of the NEAD and any associated data."[7]

4. *The NEAD Privacy and Security Plan*. Following the release of the *Indoor Location Fourth Report and Order*, CTIA, a wireless communications industry trade association, created NEAD, LLC, a non-profit entity that the National Carriers have appointed to oversee development and operation of the NEAD platform and to serve as the NEAD Administrator.[8] On February 3, 2017, NEAD, LLC and the National Carriers submitted the Plan to the Commission.

5. The Plan explains that the NEAD platform is comprised of two main components: (1) the NEAD, a database of verified wireless access point street address information described above, and (2) the National Emergency Address Manager (NEAM).[9] The NEAM is a set of systems that will receive, process, and verify information on wireless access points that are submitted for inclusion in the NEAD.[10] When a caller dials 911 from his or her wireless handset equipped with Wi-Fi and/or Bluetooth radios, the participating wireless carrier network will automatically collect information from the wireless handset about wireless access points within the vicinity of the wireless handset.[11] The wireless carrier network will query the NEAD platform to determine whether the MAC address or BT-PDA information of any of these wireless access points is in the NEAD and is associated with a verified street address. If so, the wireless carrier network will provide street address information, as well as other in-building location information, to the PSAP as part of the 911 call.[12] The Plan provides that during the call, "[a] 911 caller's

[4] *Indoor Location Fourth Report and Order*, 30 FCC Rcd at 1285, para. 71; 47 CFR § 20.18(i)(4)(iv) (before using the NEAD, "CMRS providers must certify that they will not use the NEAD or associated data for any non-911 purpose, except as otherwise required by law").

[5] *Indoor Location Fourth Report and Order*, 30 FCC Rcd at 1284-85, paras. 69-70; *see also* 47 CFR § 20.18(i)(4)(iii). In response to concerns raised about the privacy and security of the NEAD database information that they had proposed, the National Carriers "commit[ed] to require the vendor(s) selected for the NEAD administration to develop a Privacy and Security Plan in advance of going live and transmit it to the FCC." Letter from Joan Marsh, AT&T Services, Inc.; Ray Rothermel, Sprint; Kathleen O'Brien Ham, T-Mobile USA; Kathleen Grillo, Verizon to Marlene H. Dortch, Secretary, FCC, PS Docket No. 07-114 at 4 (filed Jan. 21, 2015).

[6] *Indoor Location Fourth Report and Order,* 30 FCC Rcd at 1285, para. 70.

[7] *Id*.

[8] *See* Cover Letter at 1; *see also* 47 CFR § 20.18(i)(4)(iii) (NEAD Administrator "will serve as a point of contact for the Commission and shall be accountable for the effectiveness of the security, privacy, and resiliency measures" of the plan). Each of the National Carriers is a member of CTIA.

[9] *See* Plan at 1.

[10] *Id*. at 3.

[11] *Id*. at 2.

[12] *Id*.

name and telephone number will not be shared with the NEAD Platform," and that the only information wireless carriers will share with the NEAD platform are "the MAC addresses of detected Wi-Fi access points and the BT-PDA information of detected Bluetooth beacons."[13]

6. The Plan states that the NEAD platform must be populated with reliable and verified wireless access point information, including street address information and MAC address or BT-PDA information, so that wireless carriers can identify a dispatchable location.[14] According to the Plan, the NEAD will initially be populated with such access point information from the National Carriers' own Wi-Fi and Bluetooth installations, and from the installations of certain other businesses solicited by the National Carriers (i.e., businesses that have established large numbers of wireless access points, such as internet service providers, hotels, restaurants, retail stores, and building managers).[15]

7. In the future, after modifications to the NEAD platform, information will also come from individual consumers, "who will be able voluntarily to input information about their wireless access points not otherwise provided to the NEAD along with information necessary for verification."[16] Data in the NEAD platform from the wireless carriers and other businesses will not include information about any associated individual consumers, such as the 911 caller's name or telephone number.[17] However, when the NEAD platform begins accepting voluntarily submitted access point data from individual consumers, those individuals "may need to provide additional information such as their name for verification purposes."[18] The Plan states that "in those cases where individual consumers do voluntarily submit access point data and their personal information to the NEAD for verification purposes, the individual consumer's personal information will not be shared, except as otherwise required by law."[19]

8. The Plan describes "comprehensive controls" to support the security and resiliency of the NEAD platform.[20] The administrative, physical, and technical controls the drafters of the Plan have selected are drawn from the leading cybersecurity frameworks and standards, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework, the International Organization for Standardization (ISO) 27001 Information Security Management Standard, the Commission's Communications Security, Reliability and Interoperability Council (CSRIC) IV Working Group 4 Report, and Center for Internet Security (CIS) Critical Security Controls.[21] The Plan also provides that administrative controls will include policies and procedures for personnel, such as background checks for all personnel with access to the NEAD platform.[22] Physical controls will include employee and personnel security procedures, badge access to facilities, biometric access to sensitive areas, as well as various perimeter defenses and continuous physical security patrol and facility monitoring.[23] Technical controls

[13] *Id*. at 4.

[14] *Id*.

[15] *Id*. at 3.

[16] *Id*.

[17] *Id*. at 4.

[18] *Id*.

[19] *Id*. The Plan further provides that once the NEAD Platform begins accepting consumer information, "[a] privacy notice will be posted on the public-facing portal of the NEAD platform, so that individual consumers who interact with the NEAD Platform to upload wireless access point information can learn about, among other things, how personal information that may be collected (e.g. name for verification and access purposes) will be used." *Id.*

[20] *Id*. at 5-7.

[21] *Id*. at 5.

[22] *Id*. The Plan also provides for enhanced background checks for personnel with higher levels of access to sensitive information.

[23] *Id*.

will include "multiple layers of protection based on applicable industry practices and standards, from the host to the network edge, as well as vulnerability scanning and penetration testing."[24] NEAD Administrator personnel involved in the operation of the NEAD platform will receive privacy and security training at least annually.[25] In addition, the Plan states that the NEAD platform will undergo privacy and cybersecurity risk assessments "at least annually."[26] The Plan notes that the NEAD is being designed to deliver "99.999% availability," that it will be supported by multiple data centers across the country, and "[i]n the event of total destruction or catastrophic failure of the core site, other core sites will provide necessary processing until restoration is achieved."[27] The Plan also describes the consumer privacy protections that will be incorporated into the operation of the NEAD platform, including provisions implementing the Commission's requirement that the information in the NEAD must be used to support the provision of E911 services and not for commercial purposes.[28]

9. On February 28, 2017, the Commission's Public Safety and Homeland Security Bureau (Bureau) released a Public Notice seeking comment on the Plan.[29] Nine parties filed comments in response to the Public Notice.[30]

III. DISCUSSION

10. As discussed below, we find that the measures proposed in the Plan are consistent with the requirements outlined in the *Indoor Location Fourth Report and Order* and address the need to protect the privacy, security, and resiliency of the NEAD.

11. In the *Indoor Location Fourth Report and Order*, the Commission stated that it expected the nationwide wireless carriers to develop the NEAD privacy and security plan in close collaboration with a broad range of stakeholders, including network security and reliability experts, equipment manufacturers, public interest advocacy groups, and non-nationwide communications service providers.[31] The Commission also noted that the nationwide carriers have pledged to collaborate with industry experts on privacy and security to "ensure that best practices are followed in the development and operation of the [NEAD] database."[32]

12. We find that the Plan submitted by the National Carriers and the NEAD, LLC has been developed consistent with these expectations. The Plan states that it was developed in consultation with CTIA's 911 Location Accuracy Advisory Group, which is comprised of organizations representing public safety professionals, individuals with disabilities, privacy experts, state and local governments, and other industry stakeholders.[33] The Plan also states that it was reviewed by public interest, consumer, and

[24] *Id*.

[25] *Id*. at 7.

[26] *Id*. at 8.

[27] *Id*. at 7.

[28] *Id*. at 4-5.

[29] *See Public Safety and Homeland Security Bureau Seeks Comment on Wireless Carriers' Privacy and Security Plan for the National Emergency Address Database (NEAD)*, DA 17-203, Public Notice, 32 FCC Rcd 1471 (2017).

[30] The commenters are the National Emergency Number Association (NENA); the Center for Democracy & Technology (CDT); the National States Geographic Information Council (NSGIC); the State of Arizona 9-1-1 Program Office; Neil MacGaffey, Director of Massachusetts Bureau of Geographic Information (MassGIS); the New York State Office of Information Technology Services; the Mississippi Automated Resource Information System (MARIS); the Harrison County (MS) Board of Supervisors; and Jeff Smith.

[31] *Indoor Location Fourth Report and Order*, 30 FCC Rcd at 1285, para. 69.

[32] *Id*.

[33] *See* Plan at 2 and n.3.

privacy advocacy organizations.[34] The Plan states that "[l]eading cybersecurity methods, such as the NIST Cybersecurity Framework (v. 1.0) and the ISO 27001 Information Security Management Standard, were used in the development of controls designed to maintain the confidentiality, availability, and integrity of the NEAD Platform's networks, systems, and data."[35] In addition, the Plan states that the NEAD platform's operations will be subject to "a program of regular audits and assessments to enable ongoing governance, compliance, and risk management."[36] We note the importance of these best practices and risk management measures and remind the National Carriers and Plan Administrator that they must continue to operate the NEAD platform in accordance with all relevant privacy, security, and resiliency best practices, and all applicable law.[37]

13. The *Indoor Location Fourth Report and Order* and the Commission's rules require that the data in the NEAD and any data associated with the NEAD may not be used for any non-911 purpose, except as otherwise required by law.[38] The *Indoor Location Fourth Report and Order* also noted that "nothing in [the order] should be construed to permit any use of customer or location information stored in the NEAD in any other context."[39] The Plan includes commitments to implement these requirements, stating that the information submitted to populate the NEAD platform "will be used to support the provision of E911 services and will not be used for commercial purposes."[40] It also provides that "[e]xcept as may be required by applicable law, information contained in the NEAD Platform will not be disclosed to third parties, including government entities, other than for E911 purposes" and that the NEAD Administrator "will follow a defined procedure to assess and respond to valid governmental requests for information."[41]

14. The Plan also received support from commenters, and no commenter opposes it. The National Emergency Number Association (NENA), for example, recommends that the Plan "should be approved."[42] The Center for Democracy & Technology (CDT) similarly expresses support, stating that it is "broadly supportive" of the Plan and is pleased to see that the Plan "continues efforts to impose a blanket restriction on the use of the NEAD Platform for any commercial purpose," emphasizing that "the careful coordination and resources devoted to the NEAD Platform by wireless carriers must not be used as a backdoor to advance the sharing or selling of information for reasons other than providing emergency services."[43]

---

[34] *Id*. at 2. According to NEAD, LLC, the following such organizations reviewed the Plan prior to submission: the Center for Democracy & Technology, Public Knowledge, the American Civil Liberties Union, the National Hispanic Media Coalition, and the National Consumers League. Cover Letter at 3.

[35] Plan at 1-2. Similarly, the Cover Letter states that the administrative, physical, and technical controls for the NEAD Platform were drawn from "the leading cybersecurity frameworks and standards, including the NIST Cybersecurity Framework, the ISO 27001 Information Security Management Standard, the Commission's CSRIC IV Working Group 4 Report, and CIS Critical Security Controls." Cover Letter at 2.

[36] Plan at 2.

[37] *See* CDT Comments at 1 (expansion of the NEAD Platform over time "will require an ongoing commitment to comprehensive data security measures and may require additional financial and technical investments by wireless carriers and the NEAD Platform").

[38] *See Indoor Location Fourth Report and Order*, 30 FCC Rcd at 1285, para. 71; 47 CFR § 20.18(i)(4)(iv) (before using the NEAD, "CMRS providers must certify that they will not use the NEAD or associated data for any non-911 purpose, except as otherwise required by law").

[39] *Indoor Location Fourth Report and Order*, 30 FCC Rcd at 1286, para. 71.

[40] *See* Plan at 4.

[41] *See id*. at 4-5.

[42] NENA Reply Comments at 4.

[43] CDT Comments at 2.

15. Based on our review of the Plan and the comment record, we find that the Plan meets the requirements of the *Indoor Location Fourth Report and Order* and includes sufficient provisions to safeguard the privacy, security, and resiliency of the NEAD when it is launched.[44] Moreover, we agree with CDT's prediction that prohibiting the use of the NEAD and associated data for non-E911 purposes will help maintain public trust in the NEAD and will, in turn, help the NEAD succeed as a means of deriving dispatchable location.[45] We therefore approve the Plan and find that it fulfills the precondition established by the Commission in the *Indoor Location Fourth Report and Order* for activation of the NEAD.[46] We will continue to monitor the implementation of the Plan by the National Carriers and the NEAD, LLC, and reserve the right to take "additional measures to protect the privacy, security, and resiliency of the NEAD and any associated data"[47] should the Plan not be adhered to by the parties.

16. *NSGIC Request*. Finally, we decline to require revision of the Plan as requested by the National States Geographic Information Council (NSGIC)[48] and several state and local entities.[49] NSGIC's request, which seeks access to the database to conduct pre-validation of addresses, is inapposite to the issue of the sufficiency of the privacy and security of the Plan. NSGIC asserts that PSAPs and state, regional, and local governments should have access to the database to be able to pre-validate the data being entered in the NEAD database against their own GIS data both to ensure the NEAD data is accurate and to identify and add missing addresses and sub-address information to their own GIS databases.[50] NENA and NEAD, LLC oppose NSGIC's request. NENA states that "NSGIC seeks access to data beyond that which was contemplated at the time E9-1-1 and/or NG9-1-1 standards were developed, beyond that which was negotiated between NENA, APCO, and the four largest wireless carriers and included in the Commission's rules, and beyond that which was designed-in to the NEAD architecture."[51] NEAD, LLC agrees with NENA's comments and states that the issues raised by NSGIC "are outside the scope of the Plan and should not be addressed as part of the FCC's approval of the

[44] In this regard, the Commission has determined that the safeguards contained in the Plan are sufficient as is, without any need to add other provisions or requirements.

[45] *See* CDT Comments at 2. The *Indoor Location Fourth Report and Order* notes that some location information in the NEAD, either by itself or in conjunction with other data concerning a consumer, may constitute proprietary information protected under Section 222 of the Communications Act. *See Indoor Location Fourth Report and Order*, 30 FCC Rcd at 1285-86, para. 71 (citing 47 U.S.C. § 222). Nothing in this *Memorandum Opinion and Order* should be construed as relieving CMRS providers of their obligations with respect to the protection of proprietary information under Section 222 and the associated regulations at 47 CFR § 64.2001 et seq.

[46] *See supra* n.5.

[47] *Indoor Location Fourth Report and Order,* 30 FCC Rcd at 1285, para. 70.

[48] NSGIC Comments at 2.

[49] *See, e.g.*, State of Arizona 9-1-1 Program Office Reply Comments at 1-2; Neil MacGaffey, Director of Massachusetts Bureau of Geographic Information (MassGIS) Comments at 1; New York State Office of Information Technology Services Reply Comments at 1; Mississippi Automated Resource Information System (MARIS) Comments at 1; Harrison County (MS) Board of Supervisors Comments at 1; *see also* Jeff Smith Reply Comments at 1.

[50] NSGIC Comments at 2. NSGIC thus recommends that "pre-validation" of a NEAD dispatchable location before that location is used during a 911 call, including the location's subaddress information (such as floor or room number), "should be considered an allowable government use for 9-1-1 purposes." *Id*. NSGIC further argues that allowing PSAPs and authoritative GIS data providers to access the NEAD database outside the context of a 911 call would reduce "costly data duplication activities," because such entities work closely with other governmental agencies that also require access to dispatchable address data, and these entities could share the GIS data to confirm its accuracy. *Id*.

[51] NENA Reply Comments at 2.

Plan."[52] We agree with parties that NSGIC's request is beyond the scope of determining the sufficiency of the privacy and security of the Plan. We find that NSGIC seeks access to the NEAD in a manner that is inconsistent with the relevant standards, which support alternative data validation procedures that do not require access to NEAD data.[53] Further, as discussed above, the *Indoor Location Fourth Report and Order* and the Commission's rules prohibit the use of the NEAD and all associated data for any purpose other than responding to 911 calls, except as required by law.[54] There is no provision in the *Indoor Location Fourth Report and Order* or the rules that authorizes the NEAD to share data with state or local entities seeking to compare address databases.

IV. ORDERING CLAUSE

17. Accordingly, **IT IS ORDERED**, pursuant to Sections 1, 2, 4(i), 7, 201, 222, 251(e), 301, 303, 303(b), 303(r), 307, 307(a), and 332 of the Communications Act of 1934, 47 U.S.C. §§ 151, 152, 154(i), 157, 201, 222, 251(e), 301, 303, 303(b), 303(r), 307, 307(a), 332; the Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, 47 U.S.C. §§ 615 note, 615, 615a, 615b; and Section 106 of the Twenty-First Century Communications and Video Accessibility Act of 2010, Pub. L. No. 111-260, 47 U.S.C. § 615c, that this *Memorandum Opinion and Order* is hereby **ADOPTED**.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

[52] Letter from Matthew B. Gerst, NEAD, LLC, to Marlene H. Dortch, Secretary, Federal Communications Commission at 3 (June 2, 2017) (on file in PS Docket No. 07-114).

[53] We note that NENA points out that "there is an existing, well-documented discrepancy reporting function in NG9-1-1" that already addresses validation queries and reports when a query returns a response that a submitted civic location is invalid and that would enable the NEAD Administrator to ensure the accuracy of the information in the NEAD database. NENA Reply Comments at 3 (citing NENA: The 9-1-1 Association, Detailed Functional and Interface Standards for the NENA i3 Solution at 97, 101-02 (2016), http://c.ymcdn.com/sites/www.nena.org/resource/resmgr/standards/NENA-STA-010.2_i3_Architectu.pdf). As NENA further observes, as drafted the Plan will support both Master Street Address Guide (MSAG) validation of addresses for E911 jurisdictions and Location Validation Functions (LVF) validation of addresses for NG911 jurisdictions. *See id.* at 4.

[54] *See Indoor Location Fourth Report and Order*, 30 FCC Rcd at 1285, para. 71; 47 CFR § 20.18(i)(4)(iv).