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

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

To: The Commission

COMMENTS IN RESPONSE TO PHONE COMPANY PLAN

James Arden Barnett, Jr.
Frederick M. Joyce
Peter S. Frechette
Venable LLP
575 7th Street, NW
Washington, D.C. 20004

Attorneys for TruePosition, Inc.

Stuart Salen, General Counsel
1000 Chesterbrook Blvd.
Berwyn, PA 19312-1084

Date: December 15, 2014

TABLE OF CONTENTS

SUMMARY iii
I. STATEMENT OF INTEREST 1
II. OVERVIEW 2
III. TECHNICAL PROBLEMS WITH WIFI/BLUETOOTH 5
A. The carriers Have Previously Said that Wifi Technologies Will Not Be Useful for E911 Location Purposes 6
B. Practical Difficulties with RF Fingerprinting Database 9
C. WiFi Technology Will Not Produce a "Dispatchable Address" 10
D. Lack of Standards/Poor Location Accuracy 11
E. The Plan Benefits only VoLTE Handset Owners 12
F. WiFi vs. UTDOA Technology 13
IV. PROPOSED TESTING IS NO SUBSTITUTE FOR ACTION 15
V. THE PLAN HAS NO MEASURABLE STANDARDS 17
VI. THE PLAN'S RELIANCE ON PRIVATE CITIZENS AND BUILDING OWNERS IS ESSENTIALLY UNENFORCEABLE BY THE FCC 20
VII. THE PLAN IMPOSES 911 STATUTORY REQUIREMENTS ON UNREGULATED INTERNET SERVICE PROVIDERS 23
VIII. THE PLAN IS NOT SUPPORTED BY PUBLIC SAFETY 25
IX. THE PLAN RELIES ON RUSSIAN MILITARY SATELLITES 27
A. National Security Issues 28
B. Network Outages/Liability Issues 28
C. Economic and Trade Issues 29
X. THE PLAN VIOLATES THE APA 31
A. Lack of Adequate Notice 32
B. The Phone Company Plan is not a "Logical Outgrowth" of the NPRM 33
XI. SOME ASPECTS OF THE PLAN WARRANT FURTHER STUDY 34
CONCLUSION 35

SUMMARY

Throughout this FCC rulemaking proceeding, public safety organizations, emergency healthcare providers, and the public have stressed the need for clear standards for improving indoor wireless 911 call location accuracy and firm benchmarks for adopting those standards. These two key elements form the foundation of the Commission's indoor accuracy rules and should not be abandoned. The Commission's proposed horizontal location accuracy standards require wireless service providers to locate wireless 911 callers on the horizontal plane within 50 meters for 67 percent of indoor calls within two years and 80 percent within five years of the effective date of adoption of the rule. This standard is balanced and technically feasible, and provides critical E911 location accuracy improvements. Conversely, the carriers' Plan focuses on studying WiFi and other technologies never before used in the 911 system and commits only to much less stringent standards and timelines for horizontal location accuracy improvements.

The FCC and many public safety officials have recognized the importance of vertical ("z-axis") location accuracy. The Commission's proposal would require vertical location accuracy within three meters accuracy for 67 percent of indoor calls within three years and 80 percent within five years. The wireless carrier Plan essentially rejects vertical accuracy, providing only for its continued study. Thus, the Plan is an enormous step backward from the important standards proposed by the FCC.

While providing a "dispatchable address" is a worthy long-term goal (assuming public safety authorities can agree on its definition and effectively use that data), the carriers' Plan abandons the critical near-term improvements to the E911 system proposed by the FCC to pursue a vague, aspirational goal. As the carriers' previous statements (as well as their Plan) attest, the technologies and resources do not exist today to provide a "dispatchable address" in the way

described by the carriers. However, the technology does exist today to meet the standards proposed by the FCC.

The substitutions proposed by the carriers will replace feasible standards and firm deadlines with vague promises, additional study, and reduced accountability. Moreover, the Plan seeks to shift the responsibility of providing life-saving E911 services to private citizens, building owners, Internet service providers, and Russian satellite systems. Here again, in addition to creating national security issues, the Plan undermines the FCC's E911 public safety framework since participation by these parties would be completely voluntary. The FCC would have essentially no legal power to enforce most aspects of the Plan.

The FCC, the public safety sector, the emergency medicine community, and many technicians have thoroughly evaluated the FCC's proposed E911 indoor location standards, which have been the subject of a lengthy rulemaking proceeding resulting in a voluminous record. The same cannot be said for the carriers' Plan. The Plan was not contained in any of the carriers' Comments or Reply Comments, and subject only to a brief additional comment period. The ideas and proposals in the Plan are not fully developed, and the commentary from industry stakeholders and the public will necessarily be incomplete and inadequate, given the short time in which to comment. Given the need for a strong and immediate fix for this glaring public safety problem, the carriers' Plan does not represent a viable alternative to the fair, reasonable and feasible indoor safety standards already proposed. The standards proposed by the Commission are technically and economically feasible today and are critically necessary for the safety and well-being of everyone

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

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

To: The Commission

COMMENTS IN RESPONSE TO PHONE COMPANY PLAN

TruePosition, Inc., through its attorneys, and pursuant to section 1.415 of the FCC's rules, 47 C.F.R. § 1.415, respectfully submits these Comments in response to the Federal Communications Commission's November 20, 2014 Public Notice ("*Notice*") in the above-referenced docket.[1] In the *Notice*, the FCC's Public Safety and Homeland Security Bureau ("Bureau") asked for comments on a so-called "roadmap" or "plan" devised largely by four phone companies (hereinafter referred to as the "Roadmap" or "Plan")[2] as an alternative to the FCC's proposal for improving indoor location accuracy for wireless 911 calls.

I. STATEMENT OF INTEREST

TruePosition is an industry leader in mobile location technology, researching and creating solutions for situations that demand accurate and reliable information. The TruePosition Location Platform has been successfully deployed throughout the United States to support the FCC's Enhanced 911 ("E911") initiative. TruePosition has been designing and deploying high

---

[1] Pursuant to a Public Notice, DA 14-1794, filed by the FCC in the above-captioned proceeding on December 9, 2014, the FCC extended the deadline for filing Comments in this proceeding to December 15, 2014; hence, these Comments are timely filed.

[2] *See* Letter, John Wright, APCO International, Charles W. McKee, Sprint, Joan Marsh, AT&T Services, Inc., Kathleen O'Brien Ham, T-Mobile USA, Christy Williams, NENA-The 9-1-1 Association, Kathleen Grillo, Verizon, to Marlene H. Dortch, Secretary, Federal Communications Commission, PS Docket No. 07-114 (filed Nov. 18, 2014) ("Letter"), Attachment A, "Roadmap for Improving E911 Location Accuracy" ("Roadmap").

performance cellular geo-location solutions since 1992. TruePosition's nationwide coverage in the United States and multiple deployments worldwide provide real-world experience that is unmatched in the industry. In short, with respect to the technological questions raised by the FCC in this rulemaking proceeding and in the phone company Plan, there are few companies extant better qualified to answer them than TruePosition.

II. OVERVIEW

Throughout the FCC's E911 rulemaking proceeding, public safety organizations, emergency healthcare providers, and the public have stressed the need for clear standards for improving indoor wireless 911 call location accuracy, and firm benchmarks for adopting those standards. These two key elements form the foundation of the Commission's proposed rules and should not be abandoned. Conversely, the wireless carriers' Plan focuses on "studying" WiFi and other technologies never before used in the 911 system, and commits only to non-existent or vague timelines for any actual horizontal location accuracy improvements.

The FCC and many commenters in this proceeding have recognized the central importance of vertical ("z-axis") location accuracy. The Commission's proposal would require vertical location accuracy within three meters accuracy for 67 percent of indoor calls within three years and 80 percent within five years. The phone company Plan only provides for "evaluation" or "study" of floor level accuracy. Thus, the Plan is a decisive step backward from the important standards proposed by the FCC.

While providing what the Plan describes as a "dispatchable address" (or "civic" address) is surely a worthy long-term goal, the carriers' Plan abandons the critical near-term improvements to the E911 system proposed by the FCC that are essential to accomplishing the longer-term goal of "dispatchable address." To a person, every public safety official who has

submitted comments in this proceeding agrees that the FCC's proposed indoor accuracy standards, by at least directing emergency assistance toward the building in question, are critically needed today. By comparison, the substitutions proposed by the carrier Plan will replace feasible standards and firm deadlines with vague promises, additional studies and reduced accountability.

Attached hereto as Exhibit One is a summary chart that compares the phone company Plan to the FCC's proposed rules for indoor location accuracy. In particular, the Plan contains the following flaws which will be addressed in greater detail in these comments:

- The Plan is dangerous. It proposes that the public safety of the United States be forced to rely upon technology that does not work indoors (handset/Global Positioning Systems ("GPS") technology), or has previously failed (Observed Time Difference of Arrival ("OTDOA")),[3] or that was not designed for 911 public safety purposes (privately owned WiFi and Bluetooth networks). Indeed, just three years ago in this rulemaking proceeding, virtually all of the wireless carriers that signed onto the Plan concluded that WiFi location technology has "considerable shortcomings" and that "no vendors have even proposed using this method for E911."[4]
- The Plan would allow phone companies to spend several more years engaged in "testing," notwithstanding recent, comparable testing *using Communications Security, Reliability and Interoperability Council ("CSRIC") protocols*. The Plan substitutes vague or open-ended goals and deadlines for the FCC's specific, attainable standards.

[3] At the time of its initial failure, OTDOA was referred to as Enhanced Observed Time Difference (EOTD).
[4] *See, e.g.*, Comments of T-Mobile USA, Inc., PS Docket No. 07-114 at 16 (Jan. 19, 2011) (T-Mobile Comments).

- The Plan contains no measurable standards for indoor accuracy and abandons the FCC's achievable standards for vertical location information.
- The Plan contains no means of determining how or when the "dispatchable address" proposal would actually work. There are no requirements on the percentage of handsets that would have "dispatchable address" capabilities within a specific number of years. There are no requirements on the percentage of E911 calls that would be provided an accurate, "dispatchable address" within a specific number of years. In fact, there is no requirement to *ever* produce a single, accurate, "dispatchable address" for even one E911 call.
- For the first time and without any legal authority, the Plan would impose 911 public safety obligations on individuals, corporations and business enterprises.
- The Plan would require Internet access companies that are not subject to 911 statutory authority to be a primary provider of indoor location information.
- Given the breadth and depth of opposition to the Plan from many highly regarded public safety organizations, it is by no means a "consensus" plan.
- The plan provides no protection for the millions of consumers who live in smaller markets, since their local carriers are unlikely to ever deploy Long-Term Evolution ("LTE") networks in the near future.
- The Plan is not "technology neutral," rather, the Plan relies on specific location technologies (GNSS, OTDOA, WiFi) and Voice-over-LTE ("VoLTE") handsets for E911 location coverage. The Plan will work only for the owners of these handsets and then only in a city with a built-out LTE network and then only in those parts of the city that are blanketed with WiFi access.

- The phone company Plan relies on military satellites owned and operated by the Russian government, which raises many troubling technical and legal problems.
- For the FCC to even contemplate adopting the Plan, it will have to launch a new NPRM; as proposed, the Plan violates the Administrative Procedure Act ("APA"). The Plan faces numerous legal obstacles, including procedural challenges under the APA and in all likelihood successful jurisdictional challenges under the Communications Act.

III. TECHNICAL PROBLEMS WITH WIFI/BLUETOOTH

The Plan is inherently dangerous in that it relies on technology that either does not work indoors (handset/GPS technology), has failed in the past and never been proven to be effective for E911 (OTDOA), or that was never designed for E911 public safety purposes (WiFi/Bluetooth/WLANs). *See* Roadmap at 4-6, Section 2. While someday it may be possible to integrate low-power, unlicensed technologies such as WiFi and Bluetooth (collectively "WLAN") into the Nation's public safety networks in ways that enhance safety for everyone, today there is no evidence that these technologies can promote 911 accuracy as suggested in the Plan. There is simply no evidence in the FCC's rulemaking docket that any proposed 911 location solution based on these technologies is reliable for emergency-grade location purposes or could provide *any* reasonable degree of location accuracy.

Just three years ago, virtually all of the wireless carriers that drafted the Plan informed the FCC that "the reliability and effectiveness of this method [WiFi Proximity technology] for E911 purposes is questionable."[5] Indeed, T-Mobile, one of the drafters of the Plan, recently concluded that WiFi location technology has "*considerable shortcomings*" and that "WiFi

[5] T-Mobile Comments at 15; *see also* Verizon Comments at 16-17; CTIA Comments at 4.

Proximity methods also *share common weaknesses with A-GPS in many indoor environments* (where access points cannot readily be located and documented) . . . ."[6] There is no evidence extant to suggest that the carriers were mistaken about the limits of WiFi technology for emergency services.

Given vociferous objections by these same phone companies to the FCC's proposed indoor safety requirements, which could be achieved by modest enhancements to *existing* technologies,[7] their sudden suggestion that indoor E911 public safety should be supported by *entirely unproven WiFi technologies* is inexplicable and alarming. Highlighted below, and in the attached engineering analysis from AdGen Telecom Group,[8] are some of the many technical problems that would occur if the FCC were to adopt the phone company Plan to use unlicensed WiFi and Bluetooth technology as the foundation for indoor E911 location accuracy.

A. The Carriers have Previously Said that WiFi Technologies will <u>not</u> be Useful for E911 Location Purposes

As recently as three years ago in response to FCC questions about what could be done to enhance E911 indoor accuracy information, the same wireless carriers that created the "Roadmap" informed the FCC that "alternative technologies" such as WiFi technology would *not* be helpful in enhancing E911 location accuracy.[9] The "Roadmap" provides absolutely no explanation as to what might have happened in the brief time since then to make these carriers

---

[6] T-Mobile Comments at 15-16 (emphasis added).

[7] *See, e.g.*, Comments of AT&T, PS Docket 07-114, at 7 (May 12, 2014) (AT&T 2014 Comments) (calling the FCC's proposed standards "technologically and commercially infeasible"); Comments of Sprint Corporation, PS Docket No. 07-114, at 4 (May 12, 2014) (Sprint 2014 Comments) (stating that the FCC's proposal "cannot be met without further advancements to today's technology); Comments of T-Mobile USA, Inc., PS Docket 07-114, at 17 (May 12, 2014) (T-Mobile 2014 Comments) (arguing that current technology does not "support the 50 meter indoor benchmark"); Comments of Verizon and Verizon Wireless, PS Docket 07-114, at 12 (May 12, 2014) (Verizon 2014 Comments) (stating that the FCC's proposed benchmarks are not "technically feasible").

[8] AdGen Telecom Group, *Technical Analysis of the Roadmap for Improving E91 Location Accuracy* (Dec. 12, 2014) ("AdGen Study"), attached hereto as Exhibit Two.

[9] *See* Comments of Verizon and Verizon Wireless, PS Docket No. 07-114 at 18-19 (Jan. 19, 2011) ("Verizon Comments"); T-Mobile Comments at 15.

change their minds about the merits of unlicensed radio technology. The fact is—nothing has changed; WiFi and other unlicensed radio services remain unproven and dangerous for E911 public safety use.

Here is a detailed explanation from T-Mobile as to why using WiFi "proximity technology" is a bad idea for public safety use, and why the situation will worsen in the coming years as manufacturers increase the coverage and range of WiFi hotspots:

> WiFi Proximity methods use WiFi access points at known locations to estimate the location of a caller. This method requires a high density of WiFi access points to function, as well as a constantly maintained database of access point locations, due to the dynamic nature of WiFi networks. As a result, WiFi Proximity only works in urban and dense suburban areas, and only with phones that have WiFi-receive capability. *WiFi Proximity methods also share common weaknesses with A-GPS in many indoor environments (where access points cannot readily be located and documented)* and in heavily forested rural areas (where access point densities are low).
>
> Because the radii for WiFi access points are on the order of 100 meters, this technology can produce medium level accuracy. *However, newer WiFi technologies and standards (such as IEEE 802.11 n) are expected to extend coverage radii to several hundred meters, which will likely degrade location accuracy*.
>
> *In addition, current E911 control plane interface standards do not support the use of WiFi Proximity location estimates for E911 purposes, and developing and maintaining the required database to support this method is operationally intensive and costly. WiFi operates on unlicensed band frequencies in dynamic networks, which are unplanned, unmanaged, and contain a mix of public and private access points. Mobile and portable WiFi access points have been in use for some time (e.g., MiFi cards, smartphones with built-in WiFi access points, vehicles with access points), resulting in a growing number of access points that are not stationary. An area that is accurately calibrated today may not be accurate and reliable tomorrow. As a result, the reliability and effectiveness of this method for E911 purposes is questionable.*[10]

Sprint concurred with T-Mobile that WiFi proximity technology is unproven and not feasible for indoor location use in emergency situations.[11] Mirroring T-Mobile's technical assessment of the problems with WiFi proximity technology, Sprint told the FCC that both of the

[10] T-Mobile Comments at 15 (emphasis added).
[11] *See* Reply Comments of Sprint Nextel Corporation, PS Docket No. 07-114 at 1 (Feb. 18, 2011).

technologies proposed in the Roadmap for indoor location in emergency situations, handset-based A-GPS and unlicensed WiFi proximity technology, would not be effective for E911: "In indoor environments, global positioning system ("GPS") technologies are often unable to effectively acquire data from satellites and network technologies are constrained because signals from cell sites are often blocked by building materials. Radiofrequency ("RF") multipathing is another problem that exists in indoor environments and affects location accuracy."[12]

In short, the same carriers who drafted the Roadmap Plan have long acknowledged that handset based A-GPS and unlicensed WiFi technologies are inherently inappropriate and "unreliable" for indoor location use in emergency situations.[13] These are empirical facts. The phone company Plan would require the FCC to ignore these facts and blithely assume that at some unknown time in the future all of these well-known problems with WiFi location technology will suddenly go away. That is not a sound basis for protecting millions of American lives.

Attached to these Comments in Exhibit Two is a detailed analysis of the Roadmap, WiFi/WLAN technology, and the shortcomings of the carriers' Plan in public safety situations, conducted by the RF engineers of AdGen Telecom Group.[14] This Study confirms the view recently held by the wireless carriers—WiFi/Bluetooth technology for the likely future is and will remain inappropriate for emergency E911 purposes. To highlight just some of the many technical problems with the Roadmap's reliance on WiFi/Bluetooth technology, they include: the random location of WiFi hotspots, lack of carrier control over WiFi hotspots, interference problems with WiFi technology, lack of quality control, susceptibility to power outages, absence

[12] Sprint Reply Comments at 2 (citing Intrado Comments at 4).
[13] Verizon Comments at 16-17; CTIA Comments at 4
[14] AdGen Telecom Group, Inc., Technical Analysis of the Roadmap for Improving E911 Location Accuracy (2014) ["AdGen Study, Exhibit Two"].

of standardization, frequent relocation of WiFi hotspots, difficulties in calibrating and "fingerprinting" WiFi/Bluetooth signals, and the need to integrate WiFi location technology and public safety location standards into a sufficient number of handsets as to make this a viable, nationwide solution.[15] AdGen's Study also analyzes other technical aspects of the Roadmap and finds the phone company Plan to be largely unsupported by existing or developing radio technologies.

B. Practical Difficulties with RF Fingerprinting Database

Putting aside all of the technical problems that are inherent in unlicensed WAN technology for E911 purposes, for the phone company Plan to have any chance of being useful the carriers will have to create and maintain a completely new database that contains timely, accurate WiFi access point data for literally every access point in every building in every city in the United States. A Verizon Wireless previously warned the FCC, the carriers will have to start this WiFi mapping process from scratch, "given concerns for the accuracy and reliability of information in vendors' databases."[16] There is nothing in the Roadmap to describe how they will achieve this essential mapping process.

Indeed, prior to signing onto the Roadmap, T-Mobile explained in detail why the Roadmap's "National Emergency Address Database" and WiFi mapping concept was likely to fail. This is what T-Mobile told the FCC about the idea:

> Because RFPM methods also share common weaknesses with A-GPS in many indoor environments and in heavily forested rural areas, RF Fingerprinting is not a suitable complement to A-GPS. RF Fingerprinting has other weaknesses as well. RFPM techniques rely on careful and frequent calibration of the deployment area for any network or environment where changes regularly occur. Because such changes are common with most major network operators with large coverage areas,

[15] *See generally* AdGen Study, Exhibit Two.
[16] Verizon, Notice of Ex Parte Oral Presentation, PS Docket 07-114, at 2 (May, 18, 2011).

using RFPM would result in enormous on-going operational costs to maintain the accuracy of location estimates.[17]

The difficulties of WiFi fingerprinting are well known to the wireless carriers; however, the Roadmap does not even mention these problems, let alone explain how they will be overcome. This technique requires creation of a database known as a radio map during the calibration phase. The density of measurement samples per unit area and the accuracy of time filtering of measurements directly impact the accuracy of WLAN indoor positioning. Creating the radio map database will be an expensive, laborious, and time-consuming process; the phone company Plan grossly underestimates the difficulties involved in creating such a comprehensive database. Indeed, the Plan ignores warnings about this mapping process from at least two of the carriers that drafted the Roadmap, Verizon Wireless and T-Mobile.[18]

Due to many factors such as changes with indoor environments, let alone constant movement of WiFi access points and their owners, this database will need to be recalibrated on a regular basis. This recalibration process is not only very expensive, it is difficult to perform given the enormous number of WLAN networks owned by many different enterprises and individuals. Consequently, the actual received signal strengths (RSS) are likely to routinely differ from the records in the radio map database for some time until after this calibration or recalibration process has been completed. This calibration will have to be repeated indoors in every building every time a WiFi spot is moved or turned on.

C. WiFi Technology Will Not Produce a "Dispatchable Address"

The fundamental premise of the carrier Plan is seriously flawed: WiFi access points do *not* directly provide a dispatchable address. As T-Mobile itself has pointed out, WiFi access

[17] T-Mobile Comments at 14.
[18] *See* Verizon Comments at 6; T-Mobile Comments at 14.

points have a range of roughly 100 meters in many cases depending on their location, and with improved hardware that range could soon reach 300 meters.[19] In a typical building, a WiFi-equipped device is able to detect WiFi access points *from several neighbors*. Detection of a given WiFi access point is typically possible from many addresses; consequently, an accurate, "dispatchable address" simply cannot be mapped to a specific WiFi access point.

The phone company Roadmap contains no test data that might even hint at the possibility that WiFi or unlicensed radio beacon technology, whose signals can propagate across multiple addresses, could be employed to reliably provide an accurate "dispatchable" address. Indeed, their "Roadmap" admits that "there are no standards for use of these technologies with 9-1-1 calls."[20] This is presumably why the carrier Plan makes no commitments to provide a correct address for any 911 calls at any time in the future; there is simply no evidence at all that the proposed WiFi solution will *ever* be able to deliver a "dispatchable address."

D. Lack of Standards/Poor Location Accuracy

The phone company Plan states that it will "promote development and approval of standards within 18 months of the date of the Agreement . . . [to] allow handsets to deliver Bluetooth LE and WiFi information to the network . . . ." This is a convoluted way of admitting that WiFi/Bluetooth technology does not work today for E911 today and may not work for the foreseeable future.[21]

The unlicensed radio technologies promoted in the phone company Plan would require capabilities in mobile handsets that simply do not exist today to measure WiFi and Bluetooth signals and provide accurate location results in a control-planed solution, which is the essence of

[19] T-Mobile Comments at 15.
[20] Roadmap at 4.
[21] *Id.* at 4.

E911. These technologies also require network technology and infrastructure to support location for E911, which also do not exist today. T-Mobile has readily admitted these problems in its Comments to the FCC.[22] The carriers admit in their Roadmap that there are no existing industry standards for location accuracy that apply to any of the unlicensed radio technologies that are essential to the Plan, and they cannot tell the FCC or the public safety community if or when those standards will ever be adopted.[23]

Verizon itself warned the FCC about problems with WLAN technology, concluding that "emerging network devices have *not* provided enhanced location accuracy."[24] If these technologies cannot even "enhance" indoor accuracy, they surely cannot provide the "dispatchable address" that the Roadmap claims they will.

E. The Plan Benefits only VoLTE Handset Owners

The Roadmap suggests that under the phone company Plan only early adopters of yet-to-be-manufactured "VoLTE" handsets will see the benefits of indoor location protection for the foreseeable future.[25] Indeed, the Plan does not even hazard a guess as to what year or decade any of these handsets might be available to any consumers. That admission underscores an even more fundamental problem with the Plan: even if all of the other technical problems inherent in the Plan could be overcome, the indoor accuracy benefits of the Roadmap will be available only to those consumers who own VoLTE handsets, and even then the Roadmap will deliver indoor accuracy only in those markets that have fully-deployed LTE networks. For tens of millions of

[22] T-Mobile Comments at 15 ("[C]urrent E911 control plane interface standards do not support the use of WiFi Proximity location estimates for E911 purposes . . . .").
[23] Roadmap at 4-5.
[24] Verizon Comments at 19.
[25] Roadmap at 5, Section 2(f).

consumers in rural and suburban markets, they will *never* have reliable indoor E911 coverage in their home markets or anytime they travel into an urban area with their non-VoLTE handsets.

Moreover, the WiFi Proximity technology that the Roadmap envisions will not be available to anyone who does not own a smart-phone. WLAN-enabled technology can only be found in smart phones. While smart phones are becoming more popular among all users, not every subscriber owns one. Smartphone penetration reached 72% of the U.S. mobile subscriber market during the period ending September 2014.[26] Although it is estimated that market penetration by smart phones is likely to continue to increase in the United States, nevertheless, wireless carriers are not required to sell only smart phone devices, and there is no way of predicting when or whether smart phone usage will reach something akin to 100% in the near future.

Studies show that smart phone usage nationwide is lowest among those demographic groups, the elderly and the poor, who arguably have the highest need for E911 location services.[27] As a result, it is not practical to assume that smart phone usage, let alone VoLTE handset ownership, will be broad enough to ensure that the vast majority of Americans will have access to the Plan's indoor location technology "solutions" for years and years to come. For the vast majority of U.S. consumers, the Roadmap is a dead end for public safety.

F. WiFi vs. UTDOA Technology

TruePosition firmly believes that the FCC's E911 regulations should be "technology neutral;" nevertheless, it bears noting how a network-based indoor location solution like Uplink-

[26] comScore, *comScore-Reports-September-2014-US-Smartphone-Subscriber-Market-Share* (Nov. 6, 2104), http://www.comscore.com/Insights/Market-Rankings/comScore-Reports-September-2014-US-Smartphone-Subscriber-Market-Share.
[27] Pew Research Center, *Internet & American Life Mobile Survey* (April 3, 2012).

Time Difference of Arrival ("UTDOA") would compare to the WiFi proposal that the Roadmap envisions. In a large but typical urban area, such as New York City, for the Plan's WiFi proposal to have any chance at all of succeeding the carriers will have to do the following: accurately identify the precise locations of tens of thousands of WiFi hotspots, create a shared database for those WiFi hotspot addresses, have some way of requiring the owners of those hotspots to notify them anytime they are moved or turned off, promote new handset standards and protocols, convert all of their customers to the new standardized handsets, and then pray that WiFi technology, notwithstanding all of its interference, operational and other problems, will actually work to provide carriers with accurate indoor location information in an emergency situation.

Conversely, if the carriers installed a mere 400 UTDOA receivers at their own cellsite locations they would have blanket E911 coverage throughout essentially all of Manhattan, covering every single make and model of mobile handset in operation today, providing 50 meter horizontal accuracy well within the FCC's timeline and standards.[28] The carriers would retain complete quality control over the hardware and the data. This arrangement requires no multi-year studies, no new handsets, no experimental hardware; it does not even require the carriers to have access to the interiors of high-rise buildings. Under this scenario, the carriers would routinely obtain accurate indoor location information in accordance with the standards proposed by the FCC and requested by most public-safety answering points ("PSAPs") and public safety officials. Given these clear choices, it is difficult to understand why the phone companies suddenly view WiFi and A-GPS technology as superior solutions for the very real and pressing problem of poor indoor E911 location information.

[28] Comments of TruePosition, Inc., PS Docket No. 07-114 at 12-14 (May 12, 2014) (TruePosition Comments).

Until just a few weeks ago, nationwide wireless carriers were uniform in concluding that just about every technical proposal put forward in the Roadmap (WiFi location technology, RF mapping and A-GPS) would not work for indoor E911 location accuracy. Here is what T-Mobile concluded about the Roadmap's central premise in its previous comments to the FCC:

> In summary, the WiFi Proximity method has considerable shortcomings: limited areas of applicability, potentially low reliability, only a subset of handsets that can be located, no standards support for E911, limited accuracy, and high cost. For these reasons, though the approach has found some success as a medium accuracy location method for some commercial-location-based smartphone applications, at present no vendors have even proposed using this method for E911.[29]

There is nothing in the Roadmap, or in recent technological developments, that should cause the FCC to disagree with T-Mobile, Verizon, and the other major carriers. The Roadmap's technical plan is fundamentally flawed and should not be substituted for the FCC's proposed indoor safety rules.

IV. PROPOSED TESTING IS NO SUBSTITUTE FOR ACTION

In addition to shifting responsibility for E911 location technology to unproven WANs that are not subject to FCC jurisdiction, the phone company Plan consists largely of a variety of tests in lieu of concrete action. Section 1 of the Plan states as follows: "Carriers agree to support a test bed that will facilitate the testing of 9-1-1 location technologies that will provide information for outdoor and indoor 9-1-1 calls." Section 2 says the four phone companies will "[c]onduct a pre-standards demonstration of a dispatchable location 9-1-1 solution within 9 months from the date of the Agreement." Section 3 notes that the "[c]arriers agreed to conduct testing of OTDOA and A-GNSS (GPS and GLONASS) for both outdoor and indoor accuracy on each of their respective VoLTE platforms within 6-12 months of the Agreement . . . ." which is

[29] T-Mobile Comments at 16.

revealing given that these phone companies previously informed the FCC that they were well along toward being ready to deploy OTDOA for indoor location purposes.[30] Section 4: "Carriers agree to collect data for all live wireless 9-1-1 calls . . . ." And finally, in Section 5 of the Plan, with respect to vertical location information, the carriers state that they will "conduct and complete" various studies to see whether "there is sufficient benefit to PSAPs" to proceed with deploying technologies that will provide z-axis data.

Not unlike peeling an onion, when you strip away the various "tests" and "studies" that these four phone companies say they will conduct over the next three years, there is really nothing left. The phone company Plan entirely ignores the FCC's proposed z-axis standard while also ignoring extensive record evidence from numerous public safety officials who favor the FCC's z-axis proposal. Having aggressively promoted OTDOA technology as a panacea for problems they are having with handset technology in urban and indoor locations,[31] the phone companies now offer to do nothing but test that technology in the coming years.

The Plan also conspicuously ignores the fact that the CSRIC working group, consisting of all the major wireless carriers and many vendors, has already conducted extensive indoor location testing. TruePosition also sponsored multiple tests of indoor location technology employing CSRIC methodologies and the very engineering experts who conducted the CSRIC indoor studies.[32] These studies prove that the FCC's proposed indoor safety standards are eminently feasible with little more than minor modifications to existing technologies.[33] In light of this prior testing and analysis by the phone companies themselves, it is difficult to avoid

---

[30] T-Mobile 2014 Comments at 7 ("T-Mobile has committed financial and personnel resources to implementation of OTDOA throughout its network and is currently actively working to deploy it . . . ."); AT&T 2014 Comments at 24 ("When [VoLTE] is launched . . . handsets will begin providing [OTDOA] location estimates in places where the A-GPS technology is not available.")
[31] *See id.*
[32] TruePosition Comments at 7-12.
[33] *Id.*

concluding that the Plan is nothing more than a last-minute attempt by these phone companies to avoid fixing what is widely acknowledged as a nationwide public safety problem.

V. THE PLAN HAS NO MEASURABLE STANDARDS

The phone company Plan purports to provide "meaningful improvements and FCC-enforceable timeframes to deliver effective locations solutions."[34] The reality is that the Plan largely ignores the FCC's timetable and benchmarks for indoor location accuracy, offering instead vague or unmeasurable goals with no specific timetable for accomplishing them. It would be one thing if the Plan offered a principled basis for departing from the FCC's proposed indoor accuracy standards, such as the need for more time to accomplish even greater indoor accuracy. But, that is not the case; rather, without any public safety justification at all, the Plan simply ignores the FCC's reasonable public safety targets, substituting vague, aspirational "goals" that constitute a giant step backwards for E911 location accuracy.

For example, the Plan purports to offer public safety services a "dispatchable address" as a superior alternative to the FCC's indoor accuracy standards.[35] In fact, the phone company Plan provides no specifics as to how or when wireless carriers would be able to deliver such a thing. The Plan does provide a rough definition of "dispatchable address," that is, the "civic address of the calling party plus additional information,"[36] but other than aspiring to deliver that information someday in the future the Plan offers no specifics.

When juxtaposed against the FCC's specific indoor accuracy standards it is evident that the Plan would do *nothing* to promote indoor location accuracy. The FCC has proposed specific, two-year benchmarks for indoor horizontal accuracy: 67% of indoor wireless 911 calls must be

[34] Letter at 2.
[35] *Id.* at 1.
[36] Roadmap at 4, Section 2(a).

located within 50 meters. That data is critical and long overdue according to the many public safety officials who have participated in this rulemaking proceeding.[37]

By contrast, the phone company Plan provides no indoor-specific accuracy requirements, substituting something they call a "blended composite of indoor and outdoor" accuracy.[38] Under the phone company approach as few as 13% of all indoor wireless calls would have to be located within 50 meters, because carriers are already required to locate 67% of outdoor calls within 50 meters. Should the carriers manage to improve the accuracy of outdoor location technologies to 80% within 50 meters, they could meet their "blended" proposal without ever having to locate a single indoor 911 call.

The FCC's five-year benchmark for horizontal accuracy is similarly eviscerated under the phone company Plan through the "blending" of indoor and outdoor calls, in the section they call "metrics for assessing performance of location methods."[39] Indeed, the phone company "metrics" not only blend indoor and outdoor coverage together to meet the carriers' recommendations, the carriers' targets after year three are based entirely on "VoLTE wireless 911 calls," meaning that they would have zero obligation to include in their performance data *any* E911 calls placed by any consumers who do not happen to own a VoLTE handset (or have placed a successful E911 call using that handset). In short, if the carriers do nothing over the next five to ten years but manage to more accurately locate

[37] *See, e.g.*, Comments of the National Association of Regulatory Commissioners, PS Docket 07-114, at 8-9 (May 12, 2014) (NARUC Comments) (calling for location accuracy standards that provide "sufficient accuracy to support x-y routing"); Comments of the National Emergency Number Association, PS Docket 07-114, at 14 (May 12, 2014) (NENA Comments) ("NENA believes that the initial 50m location performance obligation, coupled with the proposed z-axis obligation, will dramatically improve the ability of public safety agencies to identify the building and floor from which a wireless 9-1-1 call originates.").
[38] For purposes of this analysis, we assume a 50-50 blend of indoor-outdoor calls.
[39] Roadmap at 8, Section 4(c).

outdoor wireless calls, under their Plan they would have no further obligation to accurately locate *any* non-VoLTE indoor wireless 911 calls.

Perhaps most surprisingly given the strong support for the FCC's vertical information standards as reflected in numerous comments filed by many public safety organizations, including one of the signatories to the phone company Plan,[40] the Plan offers no vertical accuracy standards at all. Within the three years that the public safety community would expect to see efforts by the carriers to provide floor-level accuracy under the FCC's benchmarks, the Plan instead offers an "assessment" of the situation. Ignoring the FCC's three and five year z-axis benchmarks, the phone company Plan would do nothing for the next eight years other than "evaluate options" and deliver z-axis information at some undefined time in the future only if the carriers deem that information to be "beneficial" to PSAPs.[41] In terms of z-axis specifics, in the Plan only uncompensated pressure measurements would be evaluated, even though pressure compensation to account for weather and other variables is important to achieve floor level accuracy, has already been demonstrated in CSRIC testing, and is available today from multiple vendors.

As opaque as the phone companies' indoor accuracy standards may be, their Plan would not even concede to follow the FCC's proposal for objective performance measurement under CSRIC-established standards. Instead, the carriers have proposed that compliance with their indiscernible location accuracy standards would be established through "self-validation,"

---

[40] NENA Comments at 24 ("Because there are now available multiple possible means of measuring and representing the z-axis position of a wireless 9-1-1 caller, NENA encourages the Commission to stand firm in the implementation of its proposed z-axis rules."). *See also*, Comments of the International Association of Chiefs of Police, International Association of Fire Chiefs, National Association of State Emergency Medical Services Officials, & National Sheriffs' Association, PS Docket No. 07-114, at 1-2 (Nov. 14, 2014); Ex Parte Notice of Telecommunications for the Deaf and Hard of Hearing, Inc. (TDI), National Association of the Deaf (NAD), American Association of the Deaf-Blind (AADB), Cerebral Palsy and Deaf Organization (CPADO), PS Docket No. 07-114, at 1-2 (Nov. 3, 2014).

[41] Roadmap at 10, Section 5(b).

relying on algorithm-driven "uncertainty" estimates rather than actual ground truth measurements.[42] It is understandable why so many public safety organizations are upset with this hollow proposal, particularly when it is compared to the FCC's progressive framework for indoor location accuracy.

VI. THE PLAN'S RELIANCE ON PRIVATE CITIZENS AND BUILDING OWNERS IS ESSENTIALLY UNENFORCEABLE BY THE FCC

Many commercial property, small business owners, and homeowners will no doubt be surprised to learn that the Plan could require private owners of hundreds of thousands of buildings and owners of privately owned WiFi and Bluetooth networks to cooperate with wireless carriers to meet the carriers' E911 "goals." The fact is that the FCC does not have statutory authority to impose E911 obligations on private citizens and building owners; hence, to the extent that the Plan can be fairly interpreted as having any substance at all, it is almost entirely unenforceable as a matter of law.

CTIA, the carrier's trade association, raised this very objection when the FCC proposed a similar idea for cooperation between wireless carriers and in-building Internet access entities earlier in this rulemaking proceeding. Indeed, CTIA stated categorically that the FCC lacked legal authority to enforce even a voluntary program, one based on what the FCC referred to as "governing principles," which is essentially what the Roadmap envisions. When the FCC first proposed the idea of having wireless carriers work with IP access providers to improve in-building location information for E911 just a few years ago, here is what CTIA said:

> CTIA further notes the questionable nature of the Commission's legal authority to regulate in this area. As detailed further below, the Commission deliberately acted to classify mobile broadband as an information service subject to minimal regulation, finding that doing so 'promotes our goal of ubiquitous availability of

[42] *Id.* at 8, Section 4.

> broadband to all Americans.' The regime proposed by the Commission, however, would impose considerable additional burdens on mobile broadband providers.[43]

TruePosition agrees with CTIA; the FCC has no legal authority to adopt, let alone enforce the vast majority of the ideas proposed by the wireless carriers in their Roadmap document that would require cooperation from WLAN owners and Internet access service providers. Congress has carefully crafted a nationwide 911 system aimed at delivering "rapid, efficient deployment of emergency telecommunications service . . . ."[44] The statutory framework for our Nation's 911 system was established in the *Wireless Communications and Public Safety Act of 1999*, *The Enhanced 911 Act of 2004*,[45] and *The New and Emerging Technologies 911 Improvement Act of 2008*.[46] Key provisions in these Acts of Congress are enrolled in Sections 615 and 942 of the Communications Act. These statutory provisions spell out in great detail who shall be deemed "a provider party" for purposes of 911 services, their statutory "duties" with respect to 911 services, and their statutory immunities. *See, e.g.*, 47 U.S.C. §§ 615(a), 615a-1. Mindful of advancements in communications technology and their impact on the delivery of 911 services, this statutory framework now encompasses traditional telecommunications service providers, wireless service providers, and "IP-enabled voice service providers." *Id.* § 615(b).

At the same time, Congress has imposed specific checks on the FCC's authority with regard to our Nation's 911 system. Of particular relevance to the phone company Plan, Congress has expressly stated: "Nothing in this section shall be construed to authorize or require the Commission to impose obligations or costs on any person." *Id.* § 615. The phone companies have not even attempted to explain how their Plan will get around this statutory bar.

---

[43] CTIA Comments at 6 (footnote omitted).
[44] Wireless Communications and Public Safety Act of 1999, Pub. L. 106-81, 113 Stat 1286 (Oct. 26, 1999).
[45] The Enhanced 911 Act of 2004, Pub. L. 108–494, 118 Stat 3986 (Dec. 23, 2004).
[46] The New and Emerging Technologies 911 Improvement Act of 2008, Pub. L. 110-283, 122 Stat. 2620 (July 23, 2008).

Assuming that the phone company Plan would not impose *any* costs on the owners of WiFi networks and in-building infrastructure (a dubious assumption in light of the changes necessary to make WLANs compatible with the national 911 network and the time and labor necessary to create a nationwide WLAN database), and assuming wireless carriers could recruit sufficient numbers of volunteers to make the Plan viable, there is still the question of legal liability for the owners of WLAN nodes that choose to participate in the carrier's E911 Plan.

Carriers themselves have long complained about 911 liability issues, particularly if the FCC were to require them to interconnect their licensed networks with unlicensed IP networks for purposes of E911 services. As recently as two years ago, wireless carriers complained about the liability issues that they would face if the FCC forced them to enter into the type of arrangements that the carriers are now promoting in their Roadmap. This is what the carriers told the FCC in 2011:

> [T]he Commission envisioned a situation where a potential 9-1-1 caller would receive interconnected VoIP service from one provider and broadband Internet connectivity from another provider. Indeed, a 9-1-1 call could be attempted via an application on a mobile phone that is connected over Wi-Fi or mobile broadband networks. *Such a mechanism would involve complicated interactions among VoIP providers, wireless broadband providers, and equipment manufacturers, and these parties may or may not be protected under existing sources of liability protection under federal law*.[47]

The wireless carriers have complained about potential liability issues should they be forced to connect their networks with unregulated IP networks even though they have statutory and common law immunity from liability. *See* 47 U.S.C. § 615(a). But, there is nothing in the existing statutory framework of the Communications Act that could be construed to provide comparable statutory immunity to individuals, tenants, or building owners that elect to assist the phone companies in carrying out their E911 Plan. The

[47] CTIA Comments at 10, FCC PS Docket No. 07-114 (Oct. 3, 2011) (emphasis added).

Roadmap does not even attempt to explain why all of these building owners and individuals would be willing to accept 911 liabilities that the phone companies themselves recently said they would be unwilling to accept.

If participation by enterprise-owners of WiFi networks in the wireless carriers Plan will be strictly voluntary, as at least one phone company proponent of the Plan has speculated[48] (and as seems likely given that the FCC has no authority to require any "persons" to comply with the agency's 911 regulations), that itself raises additional questions about how truly comprehensive and effective such a program will be. Moreover, the only way for private "volunteers" in the phone company Plan to be reimbursed for their expenses would be for the phone companies themselves to cover those costs since the FCC and state governments lack statutory authority to do so.

In light of all of the legal and practical difficulties involved in getting anyone to voluntarily participate in the phone company Plan, it is hard to understand why the phone companies would not simply choose to honor the FCC's proposed 911 safety regulations themselves. Under the FCC's regulations, at the very least all regulated "911 service providers" would be entitled to use state and federal 911 funds to cover at least some of their 911 costs while retaining statutory immunity for their efforts.

VII. THE PLAN IMPOSES 911 STATUTORY REQUIREMENTS ON UNREGULATED INTERNET SERVICE PROVIDERS

The phone company Plan is clear in its intent to enlist a wide variety of broadband access entities and networks as a substitute for carrier owned and operated E911 location solutions.[49]

---

[48] *See* T-Mobile Comments at 17 ("Building owners would have to be willing to permit these devices to be added to their premises, and wired into the building power systems").
[49] Letter at 2.

For this program to approach anything close to the population coverage requirements that the FCC envisioned in its FNPRM, it will require participation by essentially all of the Nation's major broadband access/Internet access service providers. Yet, just as the FCC lacks legal authority to force individual owners of WANs to participate in the phone company Plan, it also lacks authority to require broadband access companies to participate in the Roadmap's E911 Plan.

The phone company Plan fails as a matter of law for precisely the reasons that CTIA raised when it objected to a similar proposal by the FCC: the FCC lacks statutory authority to enforce it.[50] The only statutory provision that comes close to imposing 911 obligations on broadband access companies is Section 615a-1 of the Act, "Duty to provide 9-1-1 and enhanced 9-1-1 service." *See* 47 U.S.C. § 615a-1. These relatively recent amendments to the Communications Act require "IP-enabled voice service providers" to provide 9-1-1 services on demand. But, the statutory definition of "IP-enabled voice service providers" expressly refers *only* to "interconnected VOIP" services.

In other words, other than for those customers who subscribe to broadband service for interconnect VOIP services, Internet access service providers are not subject to the 911 provisions of the Communications Act. Without that statutory obligation, the phone company plan to "leverage" broadband access points is unrealistic and would be subject to successful legal challenges. It is inconceivable that all the steps necessary for the phone company Plan to accomplish indoor location accuracy—development of standards, design and manufacture of compatible devices, products and "hot-spots," creation of a secure and current address database, and interconnection with PSAPs and wireless carriers—could be accomplished without the

[50] *See* CTIA Comments at 6.

"voluntary" cooperation of essentially every Internet access service provider in the United States. However, even if they did agree to honor the phone company Plan, the FCC lacks statutory authority to enforce it.

In light of this, it is ironic that at least one of the Plan's advocates has suggested that the Roadmap was concocted so as to avoid legal challenges to the FCC's regulatory proposals.[51] The Roadmap is simply unenforceable as a matter of law. By contrast, the FCC could not be on firmer legal ground than in extending its comprehensive E911 statutory authority over licensed, commercial wireless carriers to require them to protect their customers when E911 calls are placed from indoor locations. To suggest as some have that the FCC's E911 regulatory authority stops at the sidewalk and does not extend to reasonable and prudent indoor safety requirements for commercial wireless carriers strains credulity.

VIII. THE PLAN IS NOT SUPPORTED BY PUBLIC SAFETY

Given the suggestion by the phone companies that their proposal is a "consensus approach,"[52] it bears noting that many aspects of the Plan have already been rejected by many public safety organizations. Apart from the four wireless carriers who signed on to the Plan, it is not at all apparent that the proposal has widespread support from the public safety community. For instance, NENA itself is on record in the FCC's rulemaking proceeding in strong support of the FCC's indoor accuracy timetable, the 50 meter standard, and the "z-axis" requirements.[53] Given that the phone company Plan abandons essentially all of the vertical accuracy requirements it is not clear what aspects of the Plan warranted NENA's support. Moreover, the

[51] *NENA Officials Defend 911 Location Accuracy Plan*, Telecommunications Reports (Dec.15, 2014) (quoting Trey Forgety) (stating that "[t]he agreement allows parties to 'avoid lengthy litigation.'"
[52] Letter at 1.
[53] NENA Comments at 5-6, 14-15, 20-21.

Plan was apparently never shown to APCO's and NENA's full membership, let alone subject to a member vote; hence, other than board member support, it would not be accurate for the phone companies to claim that these eminent public safety organizations are firmly on board with the Plan.

At least four major public safety groups have already publicly criticized many aspects of the phone company Plan, including the manner in which it was negotiated.[54] "We were not consulted on these negotiations and were not provided any details of the discussions until October 29, 2014," was the response to the Roadmap from the International Association of Chiefs of Police (IACP), International Association of Fire Chiefs (IAFC), National Association of State Emergency Medical Services Officials (NASEMSO) and National Sheriffs' Association (NSA) in a letter to FCC Chairman Wheeler. They went on to say, "Our organizations are disappointed that we were not consulted earlier, because we represent the leadership of the frontline first responders who are called upon to respond to 9-1-1 emergencies every day."[55]

These public safety groups have noted that the version of the Plan that was submitted to the FCC is sorely lacking in many material respects. In their letter to the FCC, these public safety groups stated as follows:

> [E]ven though we support the definition of dispatchable location as defined by the earlier roadmap draft agreement proposed by CTIA and the carriers, we have serious concerns about the details of the actual roadmap. For example, we believe that the carriers should utilize all potential technology options in determining the dispatchable location of a 9-1-1 caller using a wireless device, including technology using both compensated and uncompensated barometric pressure. The proposed

[54] *See* Telecommunications Reports, *APCO, NENA, Carriers Announce 911 Accord; Other Public Groups Refuse To Sign On* (November 14, 2014), *republished at* Nat'l Pub. Safety Telecomm. Council, *This Just In*, NPSTC.wordpress.com (Nov. 17, 2014), https://npstc.wordpress.com/2014/11/17/apco-nenacarriers-announce-911-accord-other-public-safety-groups-refuse-to-sign-on/.

[55] Joint Comments of The International Association of Chiefs of Police (IACP), the International Association of Fire Chiefs (IAFC), the National Association of State Emergency Medical Services Officials (NASEMSO), and the National Sheriffs' Association (NSA), PS Docket 07-114 (Nov. 14, 2014).

> roadmap relies on technology solutions for 9-1-1 emergencies that have never been tested in a real-world environment, including the use of in-building Wi-Fi and Bluetooth information and crowdsourcing. We urge the FCC to ensure that the carriers also use technologies that have been tested by the Communications Security, Reliability and Interoperability Council (CSRIC) in their efforts to meet requirements for providing dispatchable location."[56]

Similarly, a recent survey of over 300 public safety officials revealed widespread dissatisfaction with the phone company Plan.[57] If there is a "consensus" in the public safety sector, it is that the FCC should proceed with its proposed indoor location benchmarks and timetable; the survey states that the phone company alternative would have been voted down had these public safety officials been asked to vote on it. These and other public safety entities will surely have an opportunity to voice their opinions about the phone company Plan in the time allowed by the FCC's Public Notice. What is not open to dispute, however, is the fact the Plan does not reflect a "consensus approach" among public safety officials.

IX. THE PLAN RELIES ON RUSSIAN MILITARY SATELLITES

The Plan refers repeatedly to phone company plans to "test" and "deploy" handsets that will rely on GLONASS technology for purposes of E911 location accuracy.[58] GLONASS is a military satellite constellation owned and operated by the Russian government. The Roadmap and participating phone companies apparently plan to rely heavily on Russian military satellites to accomplish their Plan for indoor E911 location accuracy. This raises a wide range of national security, reliability, liability and economic trade issues.

---

[56] *Id.*

[57] Press Release, Find Me 911 Coalition, Survey Finds Public Safety Officials Strongly Oppose Phone Company Plan On 9-1-1 Location Accuracy (Dec. 4, 2014), *available at* http://findme911.org/news/survey-finds-public-safety-officials-strongly-oppose-phone-company-plan-on-9-1-1-location-accuracy/.

[58] Roadmap at 3, 7, 8.

A. National Security Issues

This is no minor matter. The U.S. government is already engaged in litigation over allegations that it illegally made plans to use Russian rocketry equipment in the U.S. space program, in violation of the March 16, 2014 Executive Order of the President of the United States (13,661).[59] A preliminary injunction was previously ordered in that case, wherein the Presiding Judge cited "public interest and national defense and security concerns that underlie Executive Order 13661 warrant[ing] issuance of a preliminary injunction in this case . . . ."[60] Even without an in-depth knowledge of that Executive Order, your average citizen would understand that incorporating Russian military satellites into our national public safety communications infrastructure is a really bad idea.

B. Network Outages/Liability Issues

The FCC has recently dealt with the aftermath of a multi-state-wide 911 system outage.[61] Unravelling and responding to the technical and political issues that can occur with widescale 911 system outages throughout a single state is an enormously complicated task, as this agency surely knows. With a satellite system as the potential backbone of the wireless carriers' 911 location Plan, the FCC could be contemplating the possibility of a 50-state outage at one time. Indeed, the GLONASS system has already experienced multiple "unprecedented" total network service outages.[62]

The very notion of including a foreign sovereign entity into our U.S. public safety telecommunications network would be troubling enough, even if that entity were far more

---

[59] *Space Exploration Techs. v. United States*, No. 14-354 C.(Fed. Cl. July 24, 2014)
[60] *Space Exploration Techs.*, No. 14-354 C, 3 (Fed. Cl. Apr. 30, 2014) (order issuing preliminary injunction).
[61] *See* FCC, April 2014 Multistate 911 Outage Report, PS Docket No. 14-72 (Oct. 2014), *available at* http://www.fcc.gov/document/april-2014-multistate-911-outage-report.
[62] *See The System: GLONASS Fumbles Forward*, GPS World (May 1, 2014), http://gpsworld.com/the-system-glonass-fumbles-forward.

trustworthy than the Russian government. But, Russian involvement in the U.S. public safety and emergency communications network raises a variety of liability and service quality issues. For instance, does anyone really believe that the Russian government would accept responsibility for liability in the case of negligent operation of its GLONASS system that results in harm to U.S. citizens?

Moreover, the possibility that the Russian government could intentionally inflict damage on our Nation's 911 public safety network through its military satellite system cannot be dismissed. The phone company Plan will require 24/7 availability of the Russian satellite systems to have any chance of functioning as promised. Conversely, in response to U.S. trade sanctions or even expressions of concern over Russian policies, the Russians could routinely turn off their satellite system's U.S. coverage, or more ominously "spoof" or mask their GPS signals in such a way as to intentionally send out incorrect coordinates to all U.S. mobile handsets that rely on those signals. The consequences for location accuracy in an emergency situation would be catastrophic.

Questions like these concerning service reliability, governmental accountability, and even a willingness to work with the FCC to fix 911 public safety problems, are all raised by the phone company Plan to rely on Russian satellites in their 911 public safety networks. In short, the Plan's reliance on Russian-owned satellites creates significant safety and reliability issues.

C. Economic and Trade Issues

In addition to obvious national security, reliability, and public safety problems related to the integration of Russian satellites into the U.S. emergency 911 communications system, the phone company plan to rely on GLONASS-supported handsets for indoor location accuracy

raises many troubling trade and economic issues. As TruePosition has stated throughout these rulemaking proceedings, the decision by wireless carriers to rely principally on handset technology to honor their E911 regulatory obligations was not without cost: the carriers shifted their E911 compliance costs to American consumers who pay for additional satellite technology embedded in their handsets, even if that technology does not work indoors or in urban areas in an emergency situation.

This shifting of E911 compliance costs to U.S. consumers would be exacerbated if the phone companies relied on Russian GLONASS satellites for U.S. 911 location purposes. To promote commercial development of their GLONASS satellite constellation, on August 11, 2010, Russian ministers announced a plan to introduce a 25% import duty on all GPS-capable devices, including mobile phones, unless they are compatible with GLONASS.[63] The Russian government is also planning to force all car manufacturers in Russia to make cars with GLONASS starting from 2011; this will impact all car manufacturers, including U.S. auto makers like Ford, which have car assembly facilities in Russia. This tariff will also be imposed on all mobile handsets sold to Russia; handset manufacturers will inevitably pass-through those higher costs to their customers throughout the world. In short, not only will the U.S. wireless carriers be shifting their E911 location requirements and capabilities to the Russian government, but their customers will be forced to pay Russia for these services in the form of higher handset costs and tariffs.

Other U.S. trade laws and issues with Russia raise additional legal concerns about U.S. carriers relying on Russia for E911 support. The Department of Treasury's Office of Foreign Assets Control ("OFAC") administers Ukraine-related sanctions prohibiting U.S. persons from

---

[63] *Russian Deputy PM Calls for Up To 25% Duty on GPS Navigation Devices*, The China Post (11:54 AM Aug. 12, 2010), http://www.chinapost.com.tw/business/europe/2010/08/12/268437/Russian-deputy.htm.

conducting business with Specially Designated Nationals ("SDN") or entities "owned or controlled" by SDNs, as defined by the Ukraine-related sanctions regulations codified at 31 C.F.R. Part 589. In addition, U.S. persons are prohibited from dealing in certain debt and financing with entities designated to the Sectoral Sanctions Identification list (SSI). Together, the SDN and SSI designations include major Russian defense, financial, and energy institutions as well as Russian officials and separatist leaders, creating enormous compliance problems for U.S. public safety entities as well as the wireless carriers under the Roadmap's proposals.

Meanwhile, instead of creating more U.S.-based jobs and technology opportunities here in the United States, the phone company Plan guarantees that the economic opportunities that would otherwise be available under the FCC's indoor accuracy standards will be sent overseas to the government of Russia. Even if our current trade and political situation with Russia were not so evidently bad, the outsourcing of potential U.S. 911 jobs and technology to the Russians is a profoundly dumb idea.

X. THE PLAN VIOLATES THE APA

Some proponents of the phone company Plan have publicly stated that, if adopted, it would help the FCC avoid "lengthy legal challenges" that it might otherwise face if the agency adopts the rules set forth in its NPRM.[64] The irony of that assertion is inescapable. The phone company Plan is so patently at odds with the Communications Act and the Administrative Procedure Act that even "voluntary participation" with its key elements would likely lead to considerable litigation.

By contrast, the FCC could not be on surer statutory grounds than in its efforts to require regulated telecommunications carriers to fulfill their statutory obligations with

[64] *See, e.g.,* Telecommunications Reports, *supra*, note 54.

respect to the delivery of 911 emergency services to paying customers. The voluminous record in this rulemaking proceeding supports every key component of the FCC's indoor location accuracy standards. The only coherent objection raised by the wireless carriers appears to be that they would rather not spend the time and money necessary to fix a problem that was largely of their doing: they convinced millions of customers to "cut the wireline cord" and routinely use less reliable wireless services for 911 emergency calls. If there is any legal basis for the phone companies to avoid fixing this problem, the record is conspicuously silent on that point.

By contrast, the contents of the Plan, its creation and the manner in which it has been thrust upon the public safety sector will in all likelihood create considerable legal problems for the FCC and the Plan's proponents for the foreseeable future. Just a few of the likely legal challenges to the Plan are highlighted below.

A. Lack of Adequate Notice

The FCC's November 20, 2014 Public Notice is probably inadequate as a matter of law to allow the Plan, in whole or in part, to be considered as an alternative to the FCC's proposals as outlined in the FNPRM. Although it is true that the FCC specifically sought comments on "alternative approaches" including a possible "consensus approach,"[65] interested parties in the proceedings did not have the opportunity to assess the phone companies' alternative proposals in their comments or reply comments during the rulemaking proceeding.

As a matter of law, adequate notice must allow stakeholders and members of the public to meaningfully comment on proposed rules. In *Conn. Light & Power Co. v. NRC*, 673 F.2d 525, 530-31 (D.C. Cir. 1982), the D.C. Circuit stated that "[a]n agency commits a serious

[65] FNPRM ¶ 26.

procedural error when it fails to reveal portions of the technical basis for a proposed rule in time to allow for meaningful commentary." If the actual proposals are not made available for comment during the notice-and-comment process, an agency's assertion that it will consider alternative is "too broad and unfocused to provide adequate notice[,] thus precluding meaningful comment." *See Owner-Operator Indep. Drivers Ass'n, Inc. v. Fed. Motor Carrier Safety Admin*., 494 F.3d 188, 209 (D.C. Cir. 2007) (alteration in the original). In short, if the phone companies truly intend the FCC to adopt any aspects of their Plan as an alternative to the FCC's proposed regulations, the FCC would be required as a matter of law to initiate a further notice of proposed rulemaking.

B. The Phone Company Plan is not a "Logical Outgrowth" of the NPRM

As a matter of law, final agency rules must be the "logical outgrowth" of the proposed rules, so that interested parties could have reasonably foreseen the final outcome of a rulemaking proceeding. Agencies may not make drastic changes to proposed rules without allowing sufficient time for discussion. The phone company Plan is so far removed, so obviously at odds with the regulations proposed in the NPRM that the FCC would face serious legal challenges if it were to adopt any aspect of the Plan without initiating a new notice and comment proceeding.

For example, in *Wagner Elec. Corp. v. Volpe*, 466 F.2d 1013, 1016 (3d Cir. 1972), NHTSA published a final rule that adopted the proposed strict sampling standard, but substantially downgraded the performance criteria. NHTSA defended against a "no logical outgrowth" appeal by contending that the comments filed during the notice and comment period discussed the desirability of downgrading the performance criteria. The Third Circuit rejected the agency's argument, stating that "[t]he fact that some knowledgeable manufacturers

appreciated the intimate relationship between the permissible failure rate provisions and the performance criteria, and so responded, is not relevant. Others possibly not so knowledgeable also were interested persons within the meaning of 5 U.S.C. § 553." The court emphasized that consumer groups were not given notice that the agency intended to make a tradeoff. The court therefore remanded for an additional notice and comment period.

A final rule qualifies as a logical outgrowth "if interested parties 'should have anticipated' that the change to the rule was possible, and thus reasonably should have filed their comments on the subject during the notice-and-comment period." *Ne. Md. Waste Disposal Auth. v. EPA*, 358 F.3d 936, 952 (D.C. Cir. 2004). As shown by the widespread opposition of many public safety organizations to the phone company Plan, interested parties had no reason at all to anticipate that a so-called "consensus approach" would entirely eviscerate the FCC's proposed indoor location standards. Consequently, it is difficult to discern any aspects of the Plan that could be lawfully adopted by the FCC without initiating a further notice of proposed rulemaking.

XI. SOME ASPECTS OF THE PLAN WARRANT FURTHER STUDY

There are some aspects of the phone company Plan that warrant further study by the FCC. For example, there is presumably a consensus that the ultimate goal of indoor E911 accuracy should be to achieve as accurate a location as possible as soon as possible. The Plan refers to this goal as a "dispatchable address" or "civic address." The fact is that the rulemaking record to date is not at all clear as to what "dispatchable address" means or whether that is the goal the FCC and public safety should be striving to accomplish. For instance, in recent years there have been considerable efforts at the federal level to create an

accurate, nationwide database of civic addresses; that database does not currently exist.[66] The Plan does not even mention this as a core problem; that is, if states and localities do not have an accurate, up-to-date address directory that wireless carriers and public safety officials can access, the notion of achieving a "dispatchable address" may remain elusive. Further study by the FCC of this addressable database and the currently undefined concept of "dispatchable address" is therefore warranted, while the nation moves forward with the FCC's indoor accuracy standards.

Similarly, in theory WLAN technology, if adapted to emergency communications needs, could be used to enhance the accuracy of indoor E911 location technologies. But, as the wireless carriers' themselves have noted in their comments with the FCC, there are no vendors extant that have deployed any E911 service or technology using WiFi technology.[67] A further notice of rulemaking to investigate WiFi technology and how it might be incorporated into improving E911 indoor location accuracy would be warranted, while in the meantime everyone begins working toward achieving the FCC's initial goal of 50 meter indoor accuracy.

CONCLUSION

The phone company Plan is technically and legally flawed and does not represent a "consensus"; many aspects of the Plan are opposed by a large number public safety organizations. It is by no means a sound or appropriate alternative to the FCC's eminently fair, reasonable and feasible indoor safety standards. The standards proposed by the Commission are technically and economically feasible today and are critically necessary for the safety and well-

[66] *See* National Geospatial Advisory Committee, *The Need for a National Address Database*, (Dec. 2014), *available at* http://www.fgdc.gov/ngac/meetings/december-2014/ngac-national-address-database-use-case-paper-december-2014.pdf.
[67] T-Mobile Comments at 16.

being of everyone. For these and other reasons stated by many interested parties in this rulemaking proceeding, the Commission should proceed to adopt the indoor location accuracy standards for E911 services proposed in its *Notice*.

Respectfully submitted,

_____

James Arden Barnett, Jr.
Frederick M. Joyce
Peter S. Frechette
Venable LLP
575 7th Street, NW
Washington, D.C. 20004

Attorneys for TruePosition, Inc.

Stuart Salen, General Counsel
1000 Chesterbrook Blvd.
Berwyn, PA 19312-1084

Date: December 15, 2014

EXHIBIT ONE

Comparison of FCC's Proposed Rule on Wireless 9-1-1 Location vs. Wireless Carrier-Backed Approach

	FCC's Proposed Rule	Carrier-Backed Proposal
Proposed Approach	Mandatory location accuracy requirements and timetable using existing or new technologies	Significantly delayed timetable and weakened or eliminated requirements, all dependent on new untested technologies
Requirement for "Dispatchable Addresses" for Wireless 911 Calls	No requirement	No requirement **Proposal claims to "lead" to "dispatchable address," but only specific requirement in Section 4(c) is to achieve horizontal "location accuracy performance of 50 [meters]"*
Indoor Accuracy Requirements	Specific two, three and five-year requirements for indoor location accuracy	No indoor accuracy requirements ** Under Section 4(c), accuracy measured on "blended composite of indoor and outdoor"*
Two-Year Benchmark for Horizontal Accuracy	67% of indoor wireless 9-1-1 calls must be located within 50 meters	40% of a "blended composite of indoor and outdoor" wireless 9-1-1 calls must be located within 50 meters Under blended approach, as few as 13% of indoor wireless 9-1-1 calls must be located within 50 meters, if half of all calls come from indoors ** Under existing regulations, 67% of outdoor calls must already be located within 50 meters, thus requiring only 13% of indoor calls to meet the 40% blended standard* ** If carriers improve the accuracy of outdoor location technologies to 80%, they could meet the proposed benchmark without locating a single indoor call within 50 meters*
Five-Year Benchmark for Horizontal Accuracy	80% of all indoor wireless 9-1-1 calls must be located within 50 meters	50% of a "blended composite of indoor and outdoor" wireless 9-1-1 calls must be located within 50 meters (in year three)

	FCC's Proposed Rule	Carrier-Backed Proposal
Five-Year Horizontal Benchmark (cont.)		75% of all VoLTE wireless 9-1-1 calls must be located within 50 meters ** As noted above, carriers could meet almost all of the blended standard by improving their outdoor location accuracy* ** The VoLTE-only loophole could result in complete abandonment of accuracy obligations for non-VoLTE handsets*
Three-Year Benchmark for Vertical Accuracy	3 meters for 67% of 9-1-1 calls	None ** An "assessment" to be conducted at three years with no requirements or deadlines*
Five-Year Benchmark for Vertical Accuracy	3 meters for 80% of 9-1-1 calls	None ** 6 years for some level of undefined "z-axis solution" in the top 25 cell markets* ** 8 years for some level of undefined "z-axis solution" in the top 50 cell markets*
Availability of Technology	Tested and independently verified technology available today	Proposal depends on hypothetical and unproven new database and system connecting WiFi and Bluetooth locations to physical addresses
Handsets Covered by Approach	All handsets in use today and in future	Overall handset requirement ends at 50% and could fall to zero for non-VoLTE phones Only future 4G handsets using a special, not-yet-developed VoLTE chipset will be subject to heightened performance requirement
Limitations on Type of Technology Used	Technology neutral and based on either handset or network	Long-term approach limited to handset-only system
Testing for Accuracy	Proven CSRIC approach of placing calls to compare known location with shown location	Unproven approach in which the carriers "self-validate" their accuracy based on algorithms, not actual ground truth
National Security Implications	None	Would depend on Russian GLONASS satellite system run by Russian military

EXHIBIT TWO

Technical Analysis of the Roadmap for Improving E911 Location Accuracy

Prepared by: AdGen Telecom Group, Inc.

AdGen
Advanced Generation Telecom Group Inc.

Contents

I. EXECUTIVE SUMMARY 1
II. BASIC REQUIREMENTS FOR INDOOR E911 LOCATION 2
III. WIFI LOCATION TECHNIQUES 5
A. Optimal use of WiFi for E911 Purposes 5
B. Nearest Sensor or Cell of Origin 6
C. Vendor/Enterprise Approach 7
D. Radio Fingerprinting 8
E. Propagation Modeling 10
IV. TECHNICAL PROBLEMS WITH WIFI FOR LOCATION PURPOSES 11
A. Lack of Standards 11
B. Location Accuracy Unsuited for Emergencies 11
C. Interference Problems in WiFi Networks 12
D. The Roadmap Requires VoLTE to be Used by All Wireless Carriers 13
E. Non VoLTE Handsets While Roaming into VoLTE Networks will not Work or Provide Location Information when Making E-911 Calls 14
F. WiFi Access Points – Too Few and not in Optimum Locations 14
G. WiFi Access Points are not in Service all the Time 15
H. Required Changes in Hardware and Software to Meet New Standards 16
I. Practical Difficulties with RF Fingerprinting Database 16
J. Privacy Issues can Undermine WiFi Location Technology 17
V. OTDOA AND VOLTE ARE NOT TECHNOLOGY NEUTRAL 19
VI. CONCLUSIONS 20
REFERENCES 22
AUTHOR BIOGRAPHIES 24

I. EXECUTIVE SUMMARY

AdGen Telecom Group's technical experts have reviewed the "Roadmap for Improving E911 Location Accuracy" ("Roadmap") [1] submitted to the FCC by various wireless carriers and public safety organizations, and present this technical analysis for the FCC's consideration. At its core, in an effort to provide the FCC with a technical plan for improving E911 indoor location accuracy, the Roadmap relies on a hybrid handset-based solution, which includes Observed Time Difference Of Arrival (OTDOA), Assisted Global Positioning System (A-GPS/A-GNSS), Bluetooth Low Energy Beacons, and WiFi Access Points technologies to deliver a "dispatchable address" otherwise referred to as a "civic address."

OTDOA is a feature used for location based services (LBS) which is specific to the Long Term Evolution (LTE) standard 3rd Generation Partnership Project (3GPP) Release 9. OTDOA is a methodology used in LTE networks by which the handset (a) measures the time difference received from several eNodeBs, and (b) reports the measured time differences to a Serving Mobile Location Center (eSMLC). The eSMLC uses the time differences provided by the handset and the location of the eNodeBs to estimate the location of the handset. The use of the OTDOA as an LBS requires an LTE network and upgraded handsets capable of meeting the OTDOA measurement requirements.

Other technologies that the Roadmap relies on for indoor location estimation for E911 calls are WiFi and Bluetooth. Existing applications using WiFi location technologies include indoor navigation at shopping malls, finding lost children in an indoor area, and locating lost personal property. These applications have motivated many researchers to elaborate on a number of other positioning technologies based on increasingly prevalent WiFi access points. Some companies have begun to develop commercial positioning solutions for indoor environments based on WiFi

networks. For example, in November 2011, Google announced Google Indoors, which enables indoor mapping [2].

This paper analyzes various in-building unlicensed wireless techniques and unlicensed WiFi technology to determine the Roadmap's potential for resolving poor indoor coverage for E911 location requirements. In theory, WiFi nodes should be able to enhance the accuracy of indoor E911 location technology. In practice, WiFi technology has not been developed for emergency communications use in the manner envisioned by the Roadmap. Moreover, WiFi indoor positioning technologies suffer from a number of technical factors that, absent further development by vendors and other relevant parties, would appear to limit their location estimation accuracies, such as the following:

- Complexity of radio propagation and *ad hoc* nature of infrastructures where WiFi technology resides causes multipath fading and scattering in indoor environments.
- Harmful radio interference created by other devices operating in the same unlicensed band such as Bluetooth, cordless phones, and even microwave ovens.
- Operational limitations of WiFi networks that cause significant errors.

In this Study we will address these and other technical issues related to the use of unlicensed radio technology for emergency E911 indoor location purposes.

II. BASIC REQUIREMENTS FOR INDOOR E911 LOCATION

A successful indoor location solution for E911 emergency service has to meet a number of requirements, including FCC regulatory requirements. The FCC's Notice of Proposed Rule Making (NPRM) released on March 28, 2014, seeks to expand existing E911 location requirements to include indoor location accuracy for mobile E911 calls. The basic proposed requirements are as follows [3]:

- Wireless carriers are required to provide "horizontal" indoor location accuracy that locates callers within 50 meters for 67 percent of calls within two years and 80 percent of calls within five years.
- Wireless carriers are required to provide "vertical" (i.e., floor level) indoor accuracy that locates callers within three meters for 67 percent of calls within three years and 80 percent of calls within five years.

The FCC requirements have three performance metrics: 1) the distance between the estimated location and the actual location; 2) the percentage of calls that meet the FCC accuracy requirement; and 3) the timeframe in which wireless service providers must meet the proposed indoor location requirements.

The FCC's regulatory requirements, and other operational issues that are pertinent to indoor E911 location technology, are summarized below:

- *Accuracy:* Based on the FCC requirements, the location estimation error of the indoor positioning system has to be within 50 meters horizontally and within three meters vertically.
- *Coverage:* E911 calls are unique in that each one involves urgent issues of public safety; consequently, any indoor location technology should aim to locate each call to the extent possible and relay its location to the closest PSAP.
- *Commercial availability:* The FCC's timeline for adopting indoor location requirements will require commercial availability of viable technologies in the next two to five years with appropriate accuracy and coverage.

- *Security and Privacy:* Privacy is an issue in that commercial uses of location technology should not be exploited to track an individual's position without consent. The indoor location system has to appropriately address this concern.
- *Precision and consistency:* Precision of the location system describes the consistency of the location measurement's accuracy when repeated over many trials. If for any reason the location estimations vary over time, the positioning system lacks precision and consistency.
- *Availability:* The desired indoor positioning system for E911 calls must function normally under any circumstances even during exceptional situations such as extended power outages.
- *Cost and complexity:* There is a direct relationship between cost and complexity. Complexity and cost of a location system are attributed to equipment (hardware and software), operations, calibrations and recalibrations, maintenance and testing. The complexity includes the computational complexity associated with the location estimation algorithms, especially if the algorithm is performed on the mobile device.
- *Standardization:* A successful location solution would incorporate equipment manufactured by different vendors working in an ecosystem that requires a certain degree of standardization. For example, WiFi access points (APs) manufactured by different vendors should be expected to "talk" to multiple types of handset and multiple PSAP interconnections through a standard interface.

In this Study we analyze the wireless carriers' Roadmap proposal in light of these basic engineering and operational concepts for E911 indoor location.

III. WIFI LOCATION TECHNIQUES

There are several existing and proposed indoor location techniques that employ WiFi infrastructure. This section provides an overview of these indoor location technologies. At the outset, we describe how, in ideal or optimal setting, WiFi technology would be integrated into the nation's existing E911 public safety network.

A. Optimal use of WiFi for E911 Purposes

The optimal use of WiFi technology for indoor location/public safety uses would be as follows: an E911 call in a wireless network would be routed to the local public safety answering point (PSAP) assigned to the cell that is closest to the caller's mobile device. In order for the E911 system to obtain the location of the device, some coordination between a number of network elements would be required. In an optimal, enterprise-wide WiFi setting, the E911 system would send a query to all the APs in the coverage area of the nearest cellsite (the one that serves the caller) asking if they see the mobile device in their coverage areas (Figure 1) (Note: this process would be more difficult and more complicated if multiple AP access points on a floor or in a particular building were not commonly owned or operated). Upon receiving a positive response for the query, the WiFi indoor positioning solution has to provide the location *(x,y,z)* of the mobile device. This requires a standard interface between the location server and all the WiFi APs. Also, all the WiFi APs should be able to track the Media Access Control Identifier (MAC-ID) of all the WiFi devices in their proximities.

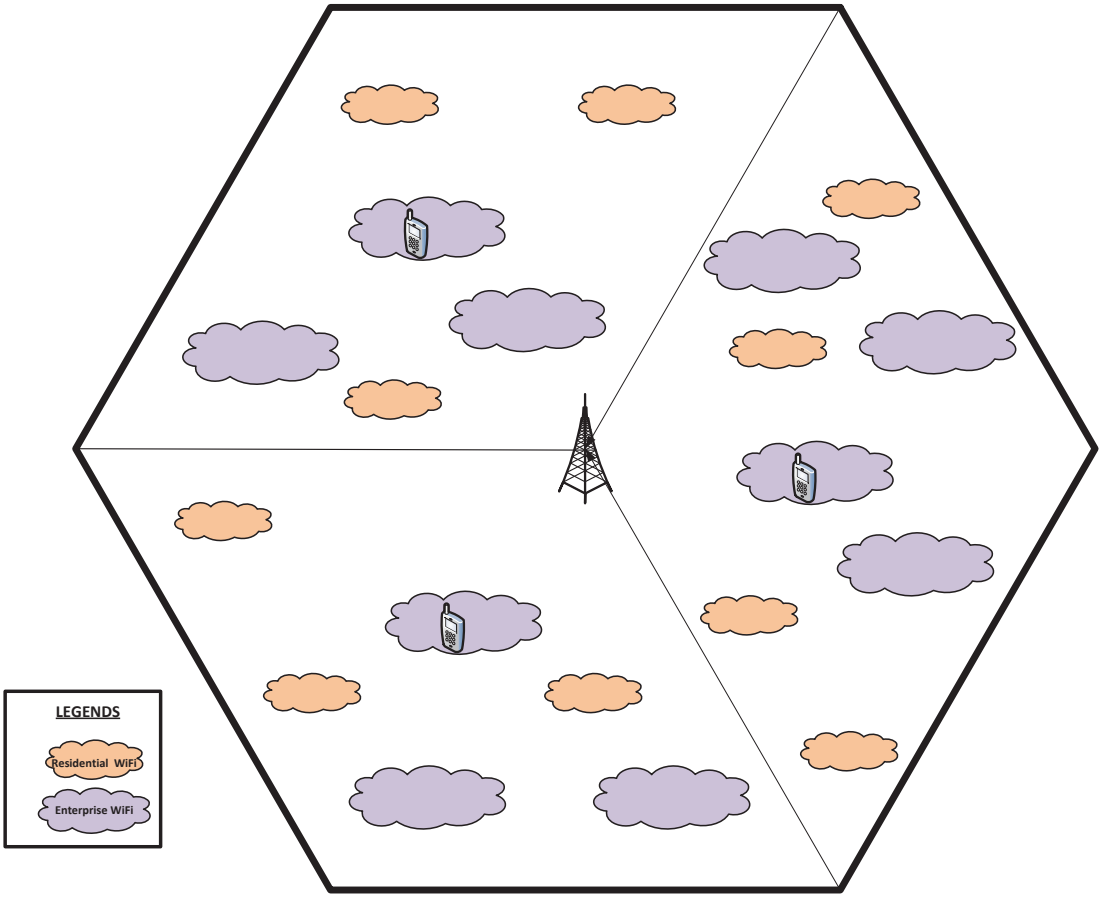

Figure 1: The E911 system sends a query to all the WiFi access points sitting in the cell that the mobile device is connected to, asking whether the mobile device is in their proximity

There are a number of technical methods whereby WiFi technology could be used to locate a mobile handset in an indoor location. Some of these technologies are already in use in various commercial settings. Depending on the particular location application, there will be different requirements for the precision of the location measurement and its degree of accuracy. In the cases of emergency calls and for public safety purposes, greater precision may be needed with greater accuracy. Chief among these WiFi-based location technologies are the following:

B. Nearest Sensor or Cell of Origin

Nearest Sensor technology or Cell of Origin technology is the simplest WiFi location method, though by itself it is the least precise. This capability, supported by most wireless network

vendors in their management systems, determines the identity of the 802.11 access point or cellular base station to which a client device (in this scenario the caller's handset) is associated. This technology assumes that the strongest sensor "heard" by the network is the closest sensor to the device; it then computes how far the handset's radio signal is from the nearest sensor.

Cell of Original location technology is the simplest positioning method to implement; however, due to its inaccuracies this technology would not be suitable for locating E911 calls. In this technology, the position of the WiFi AP in the nearby area, with the highest RSS value received at the mobile device, is identified and considered as the estimated location of the mobile device. WiFi networks have ranges of up to 100 meters; consequently, the potential margin of error for this type of WiFi location technique would routinely be 100 meters.

For the "nearest WiFi sensor" method to be useful on a wider scale it would have to be coupled with something called "RF fingerprinting" (described in greater detail below) and a comprehensive sensor database. This technique uses intelligent algorithms to improve location-tracking precision by accounting for the environmental effects - such as an object, human, mirror, windows, attenuation and multi-path - on the wireless signal. A "fingerprint" of the wireless environment is calculated by a physical walk-around using a handheld spectrum analysis device. These measurements are later compared to deviations in the real-time environment to locate the client device.

C. Vendor/Enterprise Approach

Some location-tracking technology suppliers are makers of WiFi communications systems that layer location services onto their systems. Others are third-party location specialists that provide overlay wireless tracking systems.

Vendors such as Cisco/Airespace make location technologies available on an enterprise-wide basis. These vendors can automatically calibrate a network fingerprint when they sell an office-wide system to an enterprise. Cisco claims precision of "within a few meters." This technology solution requires purchase by an enterprise of vendor-specific AP, controllers, and associated software. These enterprise solutions are not interconnected with a local PSAP, and are not controlled by the wireless service providers; consequently, many technical steps and cooperation between carriers, PSAPs and individual enterprises would be required before these WiFis could be useful E911 location accuracy.

D. Radio Fingerprinting

So-called "RF Fingerprint" positioning is the most common form of WiFi indoor positioning technique used today for commercial applications; it uses a previously created database of signal patterns to be matched for location purposes. This technology requires step-by-step empirical measurements and recording of the name and the received signal strength (RSS) of all WiFi APs at different locations throughout the entire proposed network during a calibration or training phase. The fingerprinting information is then stored in a database called a radio map. Each entry in the database is denoted as a "fingerprint" consisting of the position (x, y, z) and the RSS vector containing the empirical measurements for particular WiFi APs.

To obtain a location, the radio device (handset, laptop, etc.) measures the RSS of the nearby WiFi APs in the range. In a network-based fingerprinting system, the vector of the measured RSS of the nearby WiFi APs is sent to a location server that estimates the position of the device by correlating all RSS measurements with the RSS values of fingerprint location stored in a database (Figure 2). There are a number of pattern recognition techniques that the location server can utilize to estimate the location of the device [4].

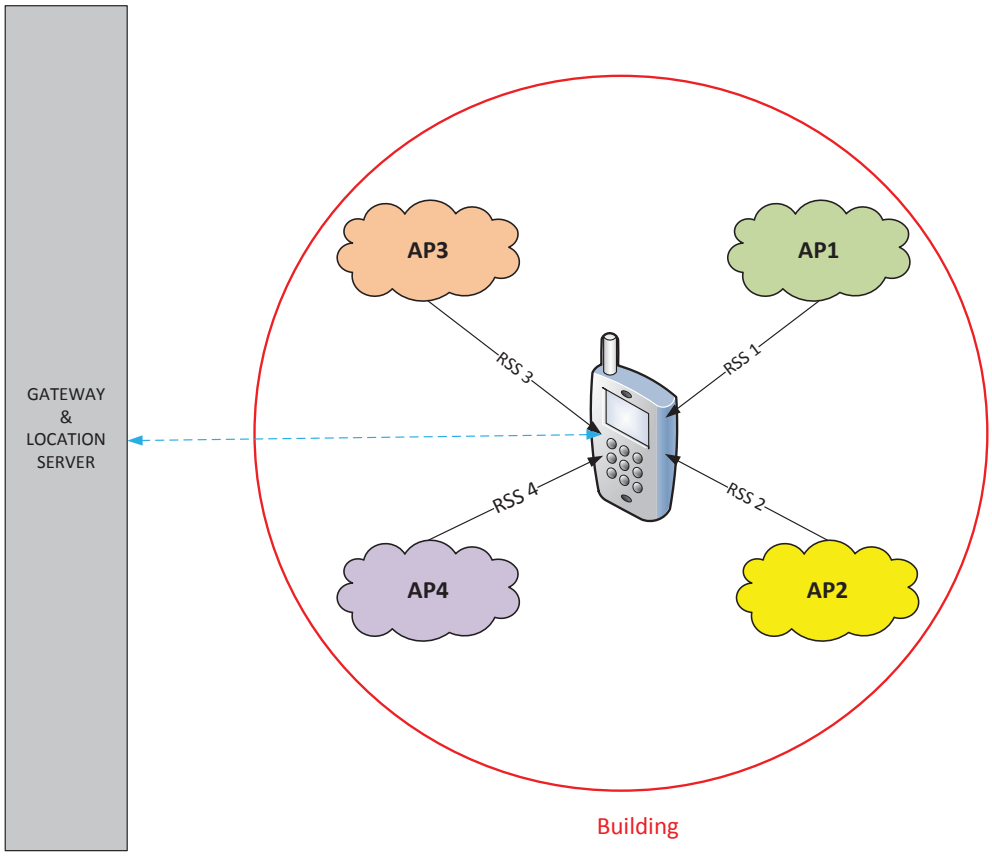

Figure 2: The mobile device measures the RSS of different WiFi APs in its proximity and sends the measured RSSs to the location server for mobile device location estimation.

Fingerprint positioning does not need any time synchronization between WiFi APs. The fingerprinting performance depends on the user's handset's orientations, the number of WiFi APs in range, the density of calibration samples where the fingerprints are taken, and effective time filtering to remove the effect of fading for each calibration sample.

WiFi indoor positioning based on fingerprinting suffers from a number of drawbacks. The main downside of WiFi fingerprinting is the expensive, laborious and time-consuming calibration process. Furthermore, this location technique is sensitive to environmental changes, such as moving of furniture, opening or closing doors, movement of people, or changing the location or operational aspects of any WiFi AP, which may necessitate recalibration of the signal strength

map. To maintain the positioning accuracy, the recalibration process should be periodically repeated to recalculate the fingerprint information. Also, the orientation or the speed of a user, or even the blockage by a user's body can contribute to changes in the RSS. Some studies reveal that blocking by a human body can reduce the RSS by as much as 15 dB [5]. This can significantly impact the accuracy of any WiFi RSS based location techniques that are based on RF fingerprinting.

There are other weaknesses with RSS based positioning techniques that can negatively impact their accuracy and usability. WiFi equipment has been designed for mid-range networking and not for location accuracy. In practice, the RSSI values collected from different chipset vendors differ in their RSS definition and characteristics. Some studies demonstrate differences of as much as 16 dB between RSSIs of different WiFi devices [6], which would adversely impact the ability of any given handset to be "located" as it travelled from one WiFi network to the next. Moreover, creating a comprehensive radio map for fingerprinting in even the smallest of geographic areas will require substantial time, labor and cost.

E. Propagation Modeling

Propagation modelling for location purposes is based on free-space path-loss [7] which relates the distance between a WiFi AP and a WiFi device by measuring the RF signal attenuation. This model is too simplistic, however, to be used for any accurate estimation of distance in indoor environments with large multi-path, scattering, reflection, refraction and absorption by the building structures. The high time-variability of signal strength in indoor environments is a main challenge for this kind of WiFi positioning technique. There are a few modified versions of this method that seek to improve the accuracy of this technique, but, they require knowledge of the thickness of walls and the dielectric properties of each wall to be useful, information which is

simply not practical for anything other than individual use within a very small, closed environment [7] [8]. In general, WiFi positioning based on propagation modeling is not very popular due to inaccuracies of the theoretical model for indoor environments; these inaccuracies make this technology inappropriate for locating E911 calls.

IV. TECHNICAL PROBLEMS WITH WIFI FOR LOCATION PURPOSES

Under optimal circumstances, WiFi technology can provide enhanced location accuracy from indoor locations. Indeed, with appropriate conditions such as those described herein, the use of WiFi technology in tandem with other forms of location technology could meet or even exceed the FCC's proposed 50 meter indoor accuracy requirements. The problem is that at present there are many technical problems that would have to be overcome to reach that level of accuracy. There simply is no WiFi proximity technology available today that would, alone or in tandem with A-GPS handset technology meet the FCC's proposed indoor accuracy requirements within the two to five year timeframe that the agency has proposed. These problems are described in detail below.

A. Lack of Standards

The unlicensed radio technologies promoted in the Roadmap would require capabilities in mobile handsets that simply do not exist today to measure WiFi and Bluetooth signals and provide accurate location results in a control-planed solution, which is the essence of E911. These technologies also require network technology and infrastructure to support location for E911, which also does not exist today. There are no existing industry standards for location accuracy that apply to any of the unlicensed radio technologies that are mentioned in the Roadmap.

B. Location Accuracy Unsuited for Emergencies

There are many technical challenges and problems that limit the accuracy of WiFi positioning technology even in commercial settings; these technical challenges would presumably

need to be overcome before WiFi proximity technology would be considered for use in the far more challenging setting of emergency/public safety situations. These challenges include large multi-path, scattering, deflections and diffractions in indoor environments, coupled with the need for frequent recalibration of a WiFi radio map database. Also, the accuracy of WiFi location techniques will be adversely impacted by a number of changing factors including the wireless device's orientation, human and physical obstructions, and differences between vendor WiFi equipment. In any sort of location/tracking application, particularly in one involving emergency situations, it is critical for the network to locate the caller's distance and coordinates from a fixed point *via* a radio frequency (RF) transmission. The WiFi positioning techniques in part estimate the location of the caller by using the received signal strength (RSS) to calculate the distance between the fixed points of the WiFi APs and the mobile device. WiFi RF signals are easily interrupted by a variety of factors including walls, furniture and human bodies that obstruct the signal path. For some purposes, such as commercial uses involving transient shoppers, these consistently unpredictable signal losses would not necessarily be problematic. WiFi signal path interference would obviously mitigate the utility of WiFi proximity technology for emergency use.

C. Interference Problems in WiFi Networks

WiFi networks share spectrum in the unlicensed band within 2.4 GHz and 5.8 GHz. This creates enormous operational difficulties and the potential for harmful interference unlike anything found with exclusive-use cellular/PCS spectrum employed by commercial wireless carriers for E911 location purposes. WiFi RF interference can be generated by any device emitting electro-magnetic signals in the same frequency band. In a WiFi network sources of harmful interference could be anything from cordless telephones to Bluetooth-enabled equipment, or even microwave ovens. The largest source of harmful interference to a WiFi network would be another WiFi

network operating in the same spectrum band; this scenario is common in virtually every commercial building in the United States, where multiple tenants operate entirely different WiFi networks from one floor to another.

Harmful interference from *any* source would have an adverse impact on the ability to obtain accurate locations, which are essential for E911 location purposes. Strong interference may cause the received signal strength not to be measured accurately, which may cause significant errors in location estimation. Unlike with exclusive-use cellular and PCS spectrum, radio interference throughout the unlicensed bands simply cannot be controlled and will create routine problems should public safety agencies be asked to rely on this technology for indoor location accuracy. So long as a given WiFi node is operated within the power limitations established by the FCC, no particular WiFi node, hotspot or enterprise system would be entitled to interference protection from another system.

D. The Roadmap Requires VoLTE to be Used by All Wireless Carriers

For the Roadmap to meet its projected timeline, it will require all wireless carriers (in addition to the four signatory nationwide wireless carriers to the Roadmap) to implement VoLTE in their networks. Although LTE has been adopted by the four nationwide carriers, it is not a technology that the remaining wireless carriers have agreed to implement in their networks within the timeline stated in the Roadmap. The implementation of LTE for other wireless carriers may not be feasible and complex due to factors such as lack of funding and lack of access to the required spectrum. The Roadmap does not include any provision for other wireless carriers who are unable or unwilling to implement LTE in their networks.

E. Non-VoLTE Handsets While Roaming into VoLTE Networks will not Work or Provide Location Information when Making E-911 Calls

The Roadmap has been developed by wireless carriers who have already agreed to implement LTE in their networks. However, the remaining wireless carriers either have not or perhaps cannot implement LTE in their networks. Wireless carriers with no plan to implement LTE and VoLTE in their networks have no incentive to upgrade their subscribers' handsets to LTE handsets with VoLTE. As a result, subscribers who subscribe to one of the wireless carriers that have not implemented LTE will likely never own a VoLTE phone; these customers will always be at risk anytime they roam into a major city where the signatories the Roadmap will be focusing their new E911 "compliance" efforts. 3G phones simply will not be recognized indoors by the wireless carriers' LTE network.

F. WiFi Access Points – Too Few and not in Optimum Locations

The placement of WiFi APs throughout a city of just about any size is essentially a random process. WiFi APs, unlike commercial wireless networks, are not designed to meet any FCC-mandated coverage standards with respect to population or geographic scope. Rather, WiFi access points are distributed throughout a given community entirely at random, their location dictated only by the specific needs of the individuals who own, lease or rent space in a particular building.

Paradoxically, from a public safety perspective sites that would be ideal locations for WiFi APs typically have few or no APs at all. For example, in and around hospitals and nursing homes concerns about radio signal interference to medical devices typically restrict the deployment of WiFi networks. Also, lower-income neighbourhoods have comparatively lower percentages of buildings with broadband, Internet-access and WiFi systems; hence, neighbourhoods that might have the greatest need for E911 services may concomitantly have the lowest levels of WiFi coverage. Many commercial and government office buildings intentionally restrict the use of

WiFi's for security reasons; many internal communications networks rely largely on fiber and broadband-based networks.

Unless WiFi APs are sufficiently dense in those areas where indoor location accuracy is particularly lacking, wireless service providers and public safety officials will be unable to obtain accurate locations using WiFi technology. The Roadmap's basic RF design concept – an indoor location network built upon a patchwork of randomly located WiFi nodes of varying quality – is at odds with basic RF network design requirements and would result in less than optimal coverage for public safety and emergency location needs.

G. WiFi Access Points are not in Service all the Time

For many reasons a WiFi AP can be out of service, such as during power outages. There are no legal or other requirements for WiFi APs to be equipped with battery backup or uninterrupted power supply (UPS). As a result, WiFi APs are susceptible to power outages, equipment failures, disconnections, floods and other catastrophic events, the very incidents that routinely generate 911 calls. The installation, maintenance and location of WiFi APs are not based on public safety factors; rather, WiFi APs are subject to the unique needs of individuals or entities that purchase and install WiFi networks. These are not carrier-grade networks and since most of them operate in non-commercial settings, there are presumably no technicians who are routinely maintaining or upgrading these unlicensed networks or individual hotspots. This is a problem for the Roadmap since the plan is to provide seamless, 24/7 indoor location information in an emergency.

H. Required Changes in Hardware and Software to Meet New Standards

For an enterprise based solution, successful use of WiFi for indoor positioning during an E911 call will require that all WiFi APs within a particular enterprise or WiFi network communicate with a distant gateway to provide information such as whether a mobile device is in proximity with a particular WiFi AP, among other things. Currently, WiFi APs do not support communication of information through any such gateway.

For enterprise based WiFi technology to work in tandem with existing E911 systems as envisioned in the Roadmap, all WiFi APs will need to be replaced with new WiFi APs capable of interfacing a gateway/location server. For a crowd sourced WiFi solution, this interface with a gateway/location servicer is not needed. Also, in order to retrieve the necessary RF fingerprint information from handsets, whether an enterprise based solution or crowd sourced, appropriate software will have to be installed on all mobile devices either manually or by changes in the handset's operating system. The interface between the mobile device and the location positioning server/system has to be defined by the standard. The standardization process is time consuming and upgrading all the WiFi APs and mobile devices will be expensive. The Roadmap does not appear to make any specific commitments as to how or when the carriers would initiate and complete this process.

I. Practical Difficulties with RF Fingerprinting Database

For the Roadmap construct to work, wireless carriers will have to create and maintain a completely new database that contains timely, accurate WiFi access point data for every floor of every building in every city in the United States. This technique requires creation of a database known as a radio map during the calibration phase. The density of measurement samples per unit area and the accuracy of time filtering of measurements directly impact the accuracy of WiFi indoor positioning. Creating the radio map database will be an expensive, laborious and time-

consuming process; the Roadmap does not explain how this process will be accomplished or in what amount of time.

Due to many factors such as changes with indoor environments, let alone constant movement of WiFi APs and their owners, this database will need to be recalibrated on a regular basis. This recalibration process is not only very expensive; it is also difficult to perform given the enormous number of WiFi networks and WiFi hotspots owned by many different enterprises and individuals. The calibration process will literally have to be performed inside every building that has WiFi access points in order for a nationwide database to be reliable; the Roadmap does not explain who will do this or how they will do this. The actual received signal strengths (RSS) are likely to routinely differ from the records in the radio map database for some time until after this calibration or recalibration process has been completed.

For this concept to work, WiFi network and individual WiFi hotspot owners, along with broadband service providers, will have to agree to voluntarily assist wireless carriers and the FCC in maintaining an accurate and up-to-date database that correctly identifies the location *(x, y, z)* of each WiFi AP.

J. Privacy Issues can Undermine WiFi Location Technology

The use of WiFi systems for E911 calls will raise privacy issues. WiFi devices by default are configured to do active scanning, but can be disabled in a radio profile. During active scans, the WiFi device always actively looks for the WiFi APs in its proximity by sending Probe-Request messages with null Service Set Identifier (SSID) name to solicit Probe-Responses from the WiFi APs, even when the user makes no attempts to connect to any WiFi networks. After receiving the Probe-Response, the WiFi device automatically connects to the preferred WiFi network. The emitted Probe-Request message from the mobile device and received by all the WiFi APs contains

the MAC-ID of the handset. Therefore, all the WiFi APs in the vicinity of the handset configured in active scans can easily track the location of the mobile device. The Roadmap makes no mention of these issues or how the carriers will deal with them.

A WiFi device configured in passive scans only listens to the beacons and Probe-Responses from the WiFi APs. Upon detecting the preferred SSID, the WiFi device connects to the preferred WiFi network. A WiFi device in passive scan does not share its MAC-ID unless it detects the preferred WiFi network. Therefore, the time the WiFi device detects and attempts to connect to the preferred WiFi, the other WiFi APs cannot track this user. Configuring the radio of WiFi device to passive scan requires the user to change certain settings on his/her WiFi device. Unless the user changes the appropriate settings, the WiFi devices with active scan can be tracked by all the WiFi APs in the close proximity of the WiFi device.

To resolve this privacy issue, many consumers can and often do reconfigure, disconnect or shutdown the WiFi capabilities in their mobile handsets. Some people may shut down the WiFi capabilities in their mobile devices to save the battery life. Obviously, if consumers do this in the context of the Roadmap's plan for indoor location tracking in an emergency, those aspect of the Roadmap that rely on WiFi proximity location technology will not work for those customers.

In addition, Apple has designed its iOS 8 so that WiFi networks and WiFi hotspots are not able to track the location of the iPhone users by sending the Probe-Request messages with random MAC-IDs during active scan. Instead, any handset or device using iOS8 will only reveal the device's location when it connects to the user's preferred WiFi network. In other words, commercial hotspot operators cannot track the position of a user who is walking nearby with an iPhone. Although the iOS 8 resolves the delicate privacy issue for the iPhone users in this

commercial setting, at the same time it undermines the use of WiFi proximity technology to locate these particular handset customers in an emergency situation

Certainly, public education campaigns could be used to educate consumers about the implications of shutting down their WiFi capabilities if WiFi proximity technology were to be routinely incorporated into the national E911 system. Nevertheless, it is worth noting that unlike the current carrier-centric E911 location systems, the integration of WiFi into this public safety network will require active participation and a certain degree of technical know-how from every user of mobile handsets. That is quite different from a carrier-centric system that can automatically locate a person in the event of an emergency so long as a battery resides within that consumer's mobile handset. If a consumer's mobile handset is not set up to receive nearby WiFi signals (because the consumer had turned off WiFi or configured it in manual WiFi scanning mode, or with iOS 8 on iPhone), whatever E911 locating capabilities that might be available from a WiFi node are rendered useless for that particular customer.

V. OTDOA AND VOLTE ARE NOT TECHNOLOGY NEUTRAL

OTDOA is a feature specified in 3GPP Release 9 standard for LTE networks. The implementation of this feature requires: (1) LTE network working on Release 9 or later, and (2) Handsets capable of measuring OTDOA.

Moreover, the implementation of VoLTE technology in a network requires the deployment of IP Multimedia Subsystem (IMS) network, which enables the LTE network to provide the control and media planes for voice service on an LTE network.

The use of IMS or even the offering of VoLTE service to customers is not mandatory or essential in LTE networks; in fact, it is expensive for the wireless carriers to deploy. Hence, it is not correct to label these methods as technology neutral.

At the same time, the Roadmap seems to assume that there is some nationwide plan for deployment of LTE networks by all wireless carriers. But, that is actually not the case; there is no nationwide plan that all of the carriers have adopted for deployment of LTE. Indeed, it is unclear as to when all carriers will ever deploy LTE and whether or not they can afford to install IMS in their networks. Consequently, those aspects of the Roadmap that rely on or assume widespread deployment of LTE and VoLTE handsets are of questionable validity.

VI. CONCLUSIONS

The Association of Public-Safety Communications Officials (APCO) International, the National Emergency Number Association (NENA) and the four national wireless carriers (AT&T Mobility, Sprint, T-Mobile USA and Verizon) have proposed a Roadmap to improve wireless E911 call location accuracy for indoor and outdoor calls. The Roadmap envisions testing of OTDOA and A-GNSS (e.g., GPS, GLONASS) and Bluetooth Low Energy Beacons, and WiFi technologies for improved outdoor and indoor location accuracy.

While in theory WiFi nodes could enhance the accuracy of indoor E911 location technology, in practice WiFi indoor positioning technologies suffer from a number of technical factors that limit their use for E911 location purposes. For one thing, successful WiFi location solutions for E911 calls will require standardization that currently does not exist. Comprehensive coverage of WiFi location also depends on a number of factors such as market penetration of smart phones.

WiFi coverage continuity, which will be critical for public safety purposes, depends on privately-owned networks that lack required monitoring and control by wireless service operators. Power outages can easily make many WiFi APs unavailable, precisely when they may be needed most during emergency situations. WiFi location solutions for E911 will require extensive

hardware and software upgrades. WiFi indoor positioning solutions rely on RF fingerprinting methods that demand regular calibration and recalibration of RF fingerprints. WiFi location solutions for E911 will require the creation of a comprehensive and costly nationwide database for WiFi APs and someone will need to regularly monitor and update that database.

Also, OTDOA requires deployment of 3GPP Release 9 by all the handsets as well as the wireless networks. The Roadmap counts on VoLTE deployment during specific period of time. Therefore, the handsets that do not support VoLTE are not covered by the Roadmap. It is not obvious whether or when a majority of handsets and wireless networks in the U.S. will be able to support VoLTE and 3GPP Release 9.

While WiFi technology has proven to be a successful solution for high-speed, mid-range data communication, it is not currently used anywhere for public safety requirements such as location of indoor E911 calls. WiFi has the potential for assisting wireless service providers in enhancing the accuracy of other indoor location technologies; but considerable work will need to be undertaken over a lengthy period of time before WiFi can be reliably incorporated into the national E911 public safety network.

REFERENCES

[1] APCO, NENA, AT&T Mobility, Sprint, T-Mobile USA, Verizon, *"Roadmap for Improving E911 Location Accuracy,"* In Response to Wireless E9-1-1 Location Accuracy Requirement, PS Docket No. 07-114, November 18, 2014.

[2] Henniges R. "*Current Approaches of WiFi Positioning*," Service-Centric Networking Seminar WS2011/2013.

[3] Federal Communications Commission – Third Further Notice of Proposed Rulemaking: Wireless E911 Location Accuracy Requirements – February 20, 2014 – Released: February 21, 2014.

[4] Farid Z., Nordin R., Ismail M., "*Recent Advances in Wireless Indoor Localization Techniques and System*," Journal of Computer Networks and Communications, Vol. 2013.

[5] King, T., Kopf, S., Haenselmann, T., Lubberger, C. and Effelsberg, W., "*Compass: A Probabilistic Indoor Positioning System Based on 802.11 and Digital Compasses*," Proceedings of the First ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization (WiNTECH), Los Angeles, CA, USA, September 2006.

[6] Vaupel, T., Seitz, J., Kiefer, F., Haimerl, S. and Thielecke, J. (2010): "*WiFi Positioning: System Considerations and Device Calibration*," Proceedings of the 2010 International Conference on Indoor Positioning and Indoor Navigation (IPIN), September 15–17, 2010 Campus Science City, ETH Zurich, Switzerland.

[7] Parodi, B. B., Lenz, H., Szabo, A., Wang, H., Horn, J., Bamberger, J. and Obradovic J., "*Initialization and Online Learning of RSS Maps for Indoor/Campus Localization*," Proceedings of Position Location and Navigation Symposium (PLANS 06), IEEE/ION, Myrtle Beach, South Carolina pp. 24–27.

[8] Chrysikos, T., Georgopoulos, G. and Kotsopoulos, S. (2009): "*Site Specific Validation of ITU Indoor Path Loss Model at 2.4 GHz*," 10th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), June 2009, pp. 1–6.

[9] Seitz, J., Vaupel, T., Meyer, S., Gutiérrez Boronat, J. and Thielecke, J., "*A Hidden Markov Model for Pedestrian Navigation*," Proceedings of the 7th Workshop on Positioning, Navigation and Communication (WPNC' 10), Dresden, Germany.

[10] Gallagher, T., Li, B., Kealy, A., Dempster, A. and Rizos, C. (2010): "*A Sector Based Campus Wide Indoor Positioning System*," Proceedings of the 2010 International Conference on Indoor Positioning and Indoor Navigation (IPIN), September 15–17, 2010 Campus Science City, ETH Zurich, Switzerland.

[11] Y.-C. Cheng, Y. Chawathe, A. LaMarca, J. Krumm, "Accuracy Characterization for Metropolitan-scale Wi-Fi Localization," in Proc Third International Conference on Mobile Systems, Applications, and Services (MobiSys 2005), 2005.

[12] Liu H., Darabi H. Baneriee P., Liu J., "Survey of Wireless Indoor Positioning Techniques and Systems," IEEE Transactions on Systems, Man, and Cybernetics – Part C: Applications and Reviews, Vol. 37, No. 6, pp. 1067 - 1080, Nov. 2007.

[13] A. Haeberlen, E. Flannery, and et al., "*Practical Robust Localization over Large-Scale 802.11 Wireless Networks*," MobiCom, 2004.

[14] B. Li, J. Salter, A. Dempster, and C. Rizos, "*Indoor Positioning Techniques Based on Wireless-LAN*," In First IEEE International Conference on Wireless Broadband and Ultra Wideband communications, 2006.

[15] W. Meng, W. Xiao, W. Ni, and L. Xie, "*Secure and Robust WiFi Fingerprinting Indoor Localization*," IPIN, 2011.

[16] E. Martin, O. Vinyals, G. Friedland, and R. Bajcsy, "*Precise Indoor Localization Using Smart Phones*," MM, 2010.

[17] A. Parnandi, K. Le, and et al., "*Coarse in-Building Localization with Smart Phones*," Mobile Computing, Applications, and Services. 2010.

[18] M. Brunato and R. Battiti, "*Statistical Learning Theory for Location Fingerprinting in Wireless LANs*," Comput. Netw., vol. 47, pp. 825–45, 2005.

[19] C. L. Wu, L. C. Fu, and F. L. Lian, "*WLAN Location Determination in Home via Support Vector Classification*," in Proc. IEEE Int. Conf. Netw., Sens. Control, 2004, vol. 2, pp. 1026–1031.

[20] P. Bahl and V. N. Padmanabhan, "*RADAR: An in-Building RF-Based User Location and Tracking System*," in Proc. IEEE INFOCOM 2000, Mar., vol. 2, pp. 775–84.

[21] http://en.wikipedia.org/wiki/Wi-Fi_positioning_system

AUTHOR BIOGRAPHIES

Mehdi Alasti, Ph.D.

Mehdi Alasti received his PhD in the area of Wireless Communication Networks from University of Maryland at College Park in Jan 2001, with the focus on MAC Layer & Application Layer cross layer design for Integrated Voice & Data Wireless Networks. Afterwards, Dr. Alasti was one of the founders of Zagros Networks Inc., a fables semiconductor start-up company headquartered in Rockville, MD (2001 - 2003), where he worked as a Principle Engineer reporting to the VP of Engineering. From July 2003 - December 2003 Dr. Alasti joined the Electrical & Computer Engineering Department of University of Maryland as a Faculty Research Associate. From January 2004 – December 2006, Dr. Alasti joined Advanced Technology Group of Airvana Inc (www.airvana.com Chelmsford, MA) reporting to Airvana CTO and working on the next generation wireless technologies and next generation products for Airvana Inc. Dr. Alasti joined AdGen Telecom Group in 2007 and is working as a Technology Strategist consultant focusing in 4G (WiMAX) and Core Network, LTE RAN, EPC Core (security & authentication, QoS, CSFB, SRVCC, VoLTE, E911, roaming/IPX, data offloading), IMS, LTE RAN, cloud based OSS/BSS, and municipal WiFi network. Dr. Alasti has published a number of technical papers in IEEE and holds a number of patents.

Mehran Nazari

Mehran Nazari has more than 30 years of experience in the design, audit, build and operation of numerous telecommunications networks in both developed and emerging markets. He has worked with varying technologies from GSM, CDMA, UMTS and LTE to WiFi/WiMax - as a result, he has been involved in strategic planning and implementation of many different generations of telecommunications technologies and infrastructure vendors. In addition to defining technology roadmaps for start-up operations, he has assisted incumbent operators review and refine existing product and service portfolios and well as enabling platform landscapes. He has extensive background and expertise in network topology, signaling and interconnect plans between fixed networks in domestic US and intentional markets. Mr. Nazari was appointed to the Communications Security, Reliability, and Interoperability Council (CSRIC IV) in May 2013 and also is a Board member of the NG9-1-1 Institute. Mr. Nazari received his Bachelor of Science degree from George Washington University in electrical engineering.

CERTIFICATE OF SERVICE

I hereby certify that on this 15th day of December, 2014, a true and correct copy of the foregoing

Comments was served by electronic service on the following:

Chairman Thomas Wheeler
Federal Communications Commission
Attn: David Alvarez, Wireless Legal Advisor
Daniel.Alvarez@fcc.gov

Chairwoman Mignon Clyburn
Federal Communications Commission
Attn: Louis Peraertz, Legal Advisor
Louis.Peraertz@fcc.gov

Commissioner Jessica Rosenworcel
Federal Communications Commission
Attn: David Goldman, Senior Legal Advisor
David.Goldman@fcc.gov

Commissioner Ajit Pai
Federal Communications Commission
Attn: Courtney Reinhard, Legal Advisor
Courtney.Reinhard@fcc.gov

Commissioner Michael O'Rielly
Federal Communications Commission
Attn: Erin McGrath, Wireless Legal Advisor
Erin.McGrath@fcc.gov

Adm. David Simpson, Chief
Public Safety and Homeland Security Bureau
Federal Communications Commission
David.Simpson@fcc.gov

David Furth, Deputy Chief
Public Safety and Homeland Security Bureau
Federal Communications Commission
David.Furth@fcc.gov

Timothy May
Communications Manager and Project Specialist for NextGeneration 9-1-1
Public Safety and Homeland Security Bureau
Federal Communications Commission

Timothy.May@fcc.gov

David Siehl
Legal Counsel
Public Safety and Homeland Security Bureau
Federal Communications Commission
David.Siehl@fcc.gov

Dana Zelman
Legal Counsel
Public Safety and Homeland Security Bureau
Federal Communications Commission
Dana.Zelman@fcc.gov

Erika Olsen
Special Counsel
Public Safety and Homeland Security Bureau
Federal Communications Commission
Erika.Olsen@fcc.gov

Thomas Beers, Chief
Policy and Licensing Division
Public Safety and Homeland Security Bureau
Federal Communications Commission
Tom.Beers@fcc.gov

Roger Sherman, Acting Chief
Wireless Telecommunications Bureau
Federal Communications Commission
Ruth.Milkman@fcc.gov

James Schlichting
Senior Deputy Bureau Chief
Wireless Telecommunications Bureau
Federal Communications Commission
James.Schlichting@fcc.gov

Jane Jackson
Associate Bureau Chief
Wireless Telecommunications Bureau
Federal Communications Commission
Jane.Jackson@fcc.gov

Charles Mathias
Associate Bureau Chief
Wireless Telecommunications Bureau

Federal Communications Commission
Charles.Mathias@fcc.gov

John Leibovitz
Deputy Bureau Chief
Wireless Telecommunications Bureau
Federal Communications Commission
John.Leibovitz@fcc.gov

Paul Murray
Assistant Bureau Chief
Wireless Telecommunications Bureau
Federal Communications Commission
Paul.Murray@fcc.gov

Julius Knapp
Chief Engineer
Office of Engineering and Technology
Federal Communications Commission
Julius.Knapp@fcc.gov

Ron Repasi
Deputy Chief Engineer
Office of Engineering and Technology
Federal Communications Commission
Ronald.Repasi@fcc.gov

Matthew Hussey
Associate Chief for Policy
Office of Engineering and Technology
Federal Communications Commission
Matthew.Hussey@fcc.gov

Mark Settle, Chief
Policy and Rules Division
Office of Engineering and Technology
Federal Communications Commission
Mark.Settle@fcc.gov

_____ss_____
Lula Robinson