EENA NG112 Technical Committee Document

Access to 112 from Private Networks

Title:	Access to 112 from Private Networks
Version:	1.0
PublicationDate:	16-04-2015
Status of the document:	Draft For comments **Approved**

EENA asbl
info@eena.org - www.eena.org

Authors and contributors to this document

This document was written by members of EENA:

Authors	Country / Organisation
Mark J. Fletcher, ENP	US / Avaya, Inc.
Wolfgang Kampichler	AT/ Frequentis

Contributors	Country / Organisation
Tony O'Brien	EENA
Cristina Lumbreras	EENA
Ian Colville	UK/Aculab
Peter Sanders	NL/ONE2MANY

EENA asbl
info@eena.org - www.eena.org

Table of contents

EENA asbl
info@eena.org - www.eena.org

1 Executive Summary

At a very early age, we teach our children the number to call in the event of an emergency. We promote a single number, from any device, anywhere. We don't teach them about trunk access codes (typically 9 or 0 in businesses and hotels), we don't teach them about voice over IP number portability, we don't teach them all of the modern technical innovations that allow our communication devices to be accessible from nearly anywhere on the planet, while using wireless technology to connect to the Public Switched Telephone Network. All of this creates a chasm of assumption and reality.

On the positive side, intelligent private networks exist, and are a treasure trove of valuable information and environmental details, crucial to public safety agencies in the time of an emergency.

In addition to highlighting the problematic connectivity of today's networks, this paper will explore potential paths forward, utilising concepts and constructs that are commonplace in today's Internet enabled networks, and how this existing data can be utilised in a cost-efficient manner to provide public safety with critical life-saving information that is sure to reduce the time of response, increase the accuracy of that response, ultimately having a positive impact on the health and well-being of citizens.

This paper makes some practical recommendations in an attempt to raise awareness, highlight existing gaps and strengthen the legislative framework. These recommendations are as follows:

- That the European Authorities should create the necessary legal instruments to mandate the direct access to 112 by private networks. Not only that but that enforcement is required thereafter. Also the legal instruments used should mandate that location information of the caller or branch is provided similar to the normal landline location information that is received today. Competent Authorities along with the relevant stakeholders should also carry out a comprehensive study and gather data on the volumes of emergency calls from private networks.
- That National Government should ensure that any EU legal instrument is fully transposed into national law and that enforcement is carried out in full by whoever is responsible. Obligations should also fall on those who sell or utilise PBX equipment.
- That Emergency Services should ensure their staff is suitably skilled and trained to identify such private network calls using the information provided to them by the telecommunications providers and equipment vendors.
- That National Regulators should set license conditions on the relevant telecommunications network providers to ensure compliance with the direct access and location information obligations
- That PBX vendors and suppliers of PBX equipment need to ensure that access to the emergency services is provided without any barriers such as a trunk code. This also applies to employers whose employees use the equipment and to whom a duty of care applies. In addition, on-site notification to alert building staff that an emergency call has been placed and a visual display to assist and direct the emergency services when they arrive should be established.

2 Introduction

Emergencies can happen anywhere, at any time. When they do occur, citizens react by grabbing the closest communications device, and calling 112 (or whatever emergency number is known to them) for help. That device may be their home telephone, their wireless cellular telephone, or it may be the phone on the desk within their office, or in the hotel room where they are staying.

When telephone services are provided by a legacy private network, such as a Multi-Line Telephone System or Private Branch Exchange (MLTS/PBX), the location of the caller can be masked from public safety. Analog devices are unable to communicate their location information to the MLTS/PBX, and based on technology available today, only a telephone number can be sent to convey location to Public Safety officials. In today's public safety network, emergency calls are routed based upon this originating station telephone number, and it's correlating "installation address." Even worse, when the call is delivered to the Public Safety Answering Position (PSAP), that very same telephone number is utilised by the call answering equipment to look up and display to the emergency call taker, that same "installation address" information.

While this is useful in a residential environment, where a single number is representative of a physical address, and in most cases, if not all, the "installation address" is the same as the "billing address", which is the same as the "physical address" of the caller. In a commercial environment, this same fact may or may not be true. Common technology exists today that allow commercial private networks to be serviced from central locations. For example, a local business may have a central location where network and telephone facilities are housed. IP networks and technology extend those services to several branch locations within the local geography.

In addition to this is the problem of direct access. Many private networks that are found in large companies, universities, hotels etc often have a 'pre-dial' number or access code in order to open an outside line. For example, such networks require the caller to hit the digit '0' in order to place an outside call which is also the case when placing an emergency call. Not being aware of this requirement or even knowing what the 'pre-dial' number is in an emergency situation could result in several failed calls, with possibly terrible consequences.

The paradigm shift here is simple. Telephone numbers no longer equal a physical location. This simple premise is what endangers MLTS/PBX users, as the basic principle and design of the public switched telephone network for emergency calls is no longer valid.

On 31 October 2014, the Electronic Communications Committee (ECC) Report 225[1] entitled "*Establishing Criteria for the Accuracy and Reliability of the Caller Location Information in support of Emergency Services*" identified and analysed the issue of emergency calls from private networks. It recommended that:

"A procedure should be established in order to be able to pinpoint the location of calls made to emergency services within corporate networks. This could be achieved by requiring the owner of a corporate network with multiple locations connected internally to properly assist the public service provider to uniquely localise, provide timely location update and route the emergency calls to the appropriate PSAPs".

The Report also carried the results of a PSAP questionnaire on the issue where many PSAPs confirmed the existence of lack or inaccurate location information from private networks.

3 Private Networks

3.1 Call Volumes

In the US, recent reviews have shown that MLTS/PBX calls can be up to 20% of the call volume at a PSAP or Control Room. This statistic includes calls from legacy and IP systems, and can vary greatly as it is entirely dependent on local geography, as well as the level of cellular service delivered within buildings. Clearly, while more data needs to be collected on this phenomenon, changing technology, and existing indoor location accuracy challenges with cellular devices, keep this a constant moving target that needs to be closely monitored, adjusting strategies so they remain in alignment with current trends. No such data exists currently in Europe.

3.2 Private Network Specific Use Cases

Specific use cases can define specific problems in specific environments. By calling out specific industries and topologies, we can provide examples of common problems, as well as best practices in dealing with those environments. It is not our intention to single out any specific industry as being more problematic than another.

3.2.1 Hotel / Motel Lodging

Hoteliers have a unique problem. In addition to attracting business travellers who likely have been exposed to MLTS/PBX environments, and may be accustomed to dialling a trunk access code (0 or 9) before making an

[1] http://www.cept.org/ecc/groups/ecc/wg-nan/page/communication-by-wg-nan-and-pt-es-chairs-on-publication-of-ecc-report-225

outside call, their spouses and family may not. Additionally, even if they have familiarity with dialling an access code for an outside phone call, in an emergency we tend to revert to our training, and that training dictates to dial the digits 112.

Direct dialling of 112 was problematic in many older MLTS/PBX systems. Quite often, these systems required the trunk access code to determine internal calls and external calls. The modernisation of the telecommunications industry, for the most part has removed that barrier in most modern systems. Changes in public numbering plans have forced systems to collect all of the digits being dialled, analyse them for proper routing, then make a trunk selection and process the call. It is because of this, that most systems can be provisioned to allow 112 to be dialled without an access code.

While this may be a simple fix on most systems installed today, bad habits of the past still haunt us in many areas, one being MLTS/PBX programming for emergency calls.

Some have suggested that a simple placard near or on the near or on the phone reminding callers what to dial in an emergency would solve the problem. Unfortunately, we cannot rely on reactions in an emergency to include reading instructions on a telephone device for explicit details on how to place an emergency call.

3.2.2 VPN Work at Home Users

Work at home Virtual Private Network (VPN) users also create a problem for private network administrators. IP connectivity allows us to connect back into the corporate network from nearly anywhere on the planet. It is a common practice for many larger global companies to allow their workforce to work remotely from their homes. This spans multiple private industries, and has enabled the "work at home parent" phenomenon to flourish. This is enabled, primarily, through the widespread availability of broadband networks globally.

To complicate the matter, many residential services are moving to voice over IP, and a phenomenon is occurring where homeowners are "cutting the cord", and dropping traditional PSTN services offered by the local exchange carriers, in exchange for mobile coverage on their cellular provider, as most offer unlimited voice and data plans at reasonable rates.

Because of this, we no longer can count on the fact that a remote VPN telephone would not be used in case of an emergency, as it may be the only "telephone" visibly available. While we could expect an adult to understand the complexities of an Internet connected VPN telephone, we cannot make that same assumption with a child or even a spouse unfamiliar with technology.

3.2.3 VPN Road Warrior Users

Exacerbating the work at home problem, is the VPN Road warrior. This type of user also connects back to the office through VPN technology, but is often not in a residence. They may be in a hotel, a public Internet café, or anywhere else where broadband is available. From a corporate perspective, they are a remote user connecting in through the VPN. Explicit details about their location are unknown to the MLTS/PBX, nor is the device location discoverable automatically. This brings forward a unique problem where the user could be able to contribute manually their location information, however there is a risk invalidating that information.

While it is a fairly simple task to validate that the address of Starbucks in the Brussels Grand Place for example, in Belgium, the ability to verify and validate the fact that you are actually located there, simply doesn't exist in today's technology. While the ability to self report a location is valuable, we need to be cognisant of the ability for someone with bad intentions to utilise this as a tool for criminal purposes. While hoax calls to 112 already are problematic today, the IP connectivity of devices can allow this to happen at a much larger scale.

Legislative activity on location awareness needs to remain top of mind with government officials, and as this technology progresses, the legislative climate around emergency calls needs to keep pace.

3.2.4 Private Network Wireless LAN Devices

Wireless devices are becoming popular in every environment, and the private networks are no exception. Many devices are in fact "dual mode", where in addition to connecting to the cellular network, they will attach to the private network wireless LAN for both voice and data services. This can become problematic, as now you have a single device with multiple modes of connectivity, and it is unreasonable to expect the user to understand what they are connected to, and when. This creates a challenge with manufacturers, as they now

must define different capabilities in the device itself, depending on the mode that is currently active. Cellular 112 calls, beyond the scope of this document, have in place their own location determination capabilities, inherent in the cellular network. Private network wireless LAN calls, or constrained by the same confines as any other network attached device. Location discovery mechanisms can be applied to these particular devices, however it cannot be assumed that location accuracy will always be available and valid.

3.2.5 Private Network Soft Phone Devices

Private network soft phone devices are unique problem, as they contain all of the specific use cases previously defined, but may exist on any computing platform which may or may not be normally a telephone. The network connectivity challenges are no different than previously discussed, however the device itself may not identify itself to the network as a telephony end point.

3.2.6 Private Network Branch Office Users

A branch office environment, within private networks, is typically a location that is located remotely from the core facility. From a network perspective, they are often connected back to the core for data services, and with voice over IP technology becoming more prominent, voice is being delivered to the branch offices from a central data center.

During the initial rollout of centralised voice over IP services, most branch offices maintained local facilities for failover purposes as well as local survivability. With the network reliability constantly being increased, reducing potential outages, as well as the phenomena where workers in a branch office pick up and move to another location that is not experiencing a network outage, the cost, complexity of local circuits is being questioned. Many businesses are under the opinion that, if I lose network, I cannot work here, therefore I will relocate my employees to where they can work. If the location is in fact going to be closed during an outage, I don't need local survivable telephones, as employee wireless devices are suitable to coordinate the evacuation of the facility and relocation.

With the lack of local circuits, the branch office can quickly lose its autonomy as it is sharing trunks with all other branch offices, as well as the main office. Since there is no specific telephone number associated with the street address of the branch office, the ability to signal public safety the specific location becomes problematic, once again going back to the existing construct of a telephone number equalling a location, for public safety services.

To solve this problem, new entities have formed called a Voice Positioning Carrier (VPC).The value that the VPC brings, is that it exists as an emergency services carrier where the corporate private network can send emergency calls to the VPC, and the VPC in turn connects the caller with the appropriate PSAP or control room based on database records that they maintain for each telephone number of their customer base.

The value this brings is that a VPC does not have to constrain itself to any geographic or political boundaries. They can operate in a cross-border environment, and the termination of emergency calls is no longer a technical challenge, just a political and regulatory one. VPC service providers can also provide user dashboards and interfaces that allow the conveyance of self entered information, especially for users located in hotels and public areas. While support for these environments becomes critical, the regulatory climate needs to support this industry for the value that it could bring, and focus on advancing location awareness of endpoints in the public networks.

3.3 Operational Problems

3.3.1 Direct access to 112

As outlined earlier, specific challenges exist in various environments controlled by commercial private networks that provide telephony services to employees and users. Absolutely the most important component to emergency services, from any network including private networks, is access. If we cannot reach 112 services, then everything else becomes a moot point. Fortunately direct access to 112 without an access code is likely the easiest anomaly to correct, as it requires the least amount of financial resources, or physical labor.

3.3.2 Routing to call to the most appropriate PSAP

Beyond access, the location of the device is clearly the most critical component to public safety so the most appropriate resources can be dispatched to the location of the emergent event. Next, but completely reliant on the proper location, is the routing of calls to the geographically appropriate PSAP or control room. it cannot be assumed that reaching any public safety agency is better than reaching no public safety agency, as often agencies are unable to transfer calls efficiently, and critical data can be lost in the process. This is especially true when political boundaries need to be crossed, and the incident involves international resources.

3.3.3 Availability of accurate location of the caller

If emergency calls are made from a MLTX/PBX network, the location information provided to the PSAP is generally the 'installation address' of the network, which is often the head office address. If an emergency call is made from an organisation with many branches, it is generally not the branch address, which is provided to the PSAP, but rather the head office/installation address. This could have disastrous consequences for the caller as the emergency call will be routed incorrectly and/or emergency resources could be dispatched to the incorrect address because such routing and dispatch decisions are based on the address that is presented to the PSAP. .

3.4 Device Location discovery as a solution

IP enabled devices can be automatically located within the network through two primary mechanisms, Layer 2 and Layer 3 discovery. This applies to both wired and wireless devices. For WLAN environments, the location is typically tracked by access point association to provide general location resolution. Typically this level of granularity is sufficient to properly route the call and apply an ANI or ELIN that is relevant to the dispatchable address.

Layer 2 discovery entails identifying each IP device by its unique Mac address, and the relevant data switch port is attached to in the network. While this can provide very granular unique location information, it by itself is not accurate. Data switch ports are typically located in an IDF closet where patch cables attached them to the building infrastructure. Because of this, understanding the data switch port by itself is not enough detail. Very exact cable records, commonly known as a wire map database, must be defined and maintained so that they can be referenced during the location discovery phase, as well as during an emergent event to determine the location of the appropriate endpoint. Understanding that a device is plugged into data port 16 of switch A38, does little good if it is not understood where port 16 is attached to the building infrastructure.

Moves adds and changes must be explicitly tracked and updated in the database to ensure correctness and accuracy. Layer 3 discovery entails identifying each IP device by its unique IP address, and controlling the geographic topology of how IP address ranges are distributed in the network.

Historically this has been problematic to manage within the enterprise IT. Recent advances in virtual LAN technology and the ability to extend Layer 2 and Layer 3 VLANs using various fabric and shortest path bridging architectures, makes this an affordable baseline for device location management. Because devices are grouped, depending on the size of that group, additional information is typically required to correlate the users location. Layer 3 subnets can easily isolate a device to a building, a floor, or even a small zone that is easily searchable in the event of an emergency.

It is important for data network engineers to remember, and understand the 112 location discovery architecture being used in a particular facility, as their goal is to flatten the network as much as possible, to enhance application performance, but that level of flattening, puts additional operational challenges and stress on the IT staff from a location management perspective.

4 Legislative change considerations

Clearly there has been a palpable change in public opinion regarding both legacy and IP based MLTS/PBX 112capabilities, and as networks are expanding and pushing their boundaries across cities and states as well as countries and continents, the lives of citizens continue to be at risk and it is clear that the primary culprit is awareness and best practice guidelines. In addition to programs that afford customer education to businesses in IT administrators, history has been clear that without firm legislative direction, there will be little to no compliance. It is additionally clear that without penalty, there exists little to no incentive, however even the slightest hint of financial impact for noncompliance is a significant motivator for the operators of private networks to implement the technology to correct this problem, that is often already present in their architectures, but there has never been any incentive to activate the functionality.

While not as much of a concern in Europe, there is still the concern that a private network is less willing to make decisions on life safety issues where no guidance is offered by the regulatory bodies. For this reason alone, it is recommended that regulatory agencies establish a position, and publish an industry vetted best practice for those interested to follow.

In addition to this there is scope to revise Article 26 of the current 2009 Universal Services Directive[2] and the suggested text is as follows:

In Article 26.1, it currently states that:

Member States shall ensure that all end-users of the service referred to in paragraph 2, including users of public pay telephones, are able to call the emergency services free of charge and without having to use any means of payment, by using the single European emergency call number "112" and any national emergency call number specified by Member States.

EENA believes that a further paragraph (1a) is required inter alia:

1a. *Member States shall ensure that all users of private electronic communication networks are able to call the emergency services, or, where applicable, the internal emergency services, free of charge, by using the single European emergency call number "112" and any national emergency call number specified by the Member States.*

Also in Article 26.5 it currently states that:

Member States shall ensure that undertakings concerned make caller location information available free of charge to the authority handling emergency calls as soon as the call reaches that authority. This shall apply to all calls to the single European emergency call number "112". Member States may extend this obligation to cover calls to national emergency numbers. Competent regulatory authorities shall lay down criteria for the accuracy and reliability of the location information provided.

EENA believes that further clarification is needed and suggests the following text to replace the above paragraph with the bold text below reflecting the new text:

Member States shall ensure that undertakings concerned make caller location information available free of charge to the authority handling emergency calls as soon as the call reaches that authority. This shall apply to all calls to the single European emergency call number "112", ***including calls from private telecommunications networks and roaming calls****. Member States may extend this obligation to cover calls to national emergency numbers. Competent regulatory authorities shall lay down criteria for the accuracy and reliability of the location information provided.*

[2] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32009L0136&from=EN

5 Commercial Business considerations

The cost of implementing an emergency services solution within an enterprise network, has been significantly reduced through simplifying the reporting process for emergency calls within the campus. In the past, it has been a common practice to establish database records at the station level indicating to PSAP and control room operators the exact cubicle or desk where the emergency is taking place.

But in reality, that exact location information is of little value, due to access control measures placed on buildings, the unfamiliarity of building interiors by emergency first responders, in the lack of floor plans to guide them on their quest to the elusive victim.

In a severe fire, visibility can be, often is, zero meters. Understanding that a victim is located at cubicle 2C231 is of little value to a first responder who has never before been in the building. Even if they were to make an attempt, a best guess could be wrong and lead them down a path into further danger. On-site security support staff, or low-cost electronic display panels can easily be provided to disseminate important information about the location of an emergency call, to anyone that is interested. With this explicit location detail already existent in an IP enabled data environment, it becomes a simple process to extend that data over disparate networks, which can include emergency first responders, internal security, or any interested and authorized party[3]. Investing in public databases that correlate telephone numbers with physical location coordinates is counterproductive. Not because that information is not valuable to emergency responders, but because those public databases are not easily and affordably updated in real time to where the nomadic and mobile behaviour of today's private network users can be reflected when seconds matter the most.

6 PSAP considerations

The role for the PSAP in private networks is one of education and best practice support. By nature their role and job description is not often understood by the public. Because of that, network engineers come up with their own logic on how things work. It is important for public safety control rooms to establish a liaison officer that can understand the challenges of the public safety community, as well as the basic challenges businesses face in the operation of their environment and networks. Being able to speak "both languages" is an acquired skill, however it does bring both sides of the table together, and sensible plans can be laid out in established that are in agreement with the mission statements of both entities.
Just as public safety engages in programs teaching children to dial 112, and how to spot an emergency and react accordingly, additional programs for business IT staff need to be developed and presented to the business community. This will increase the level of cooperation, in the level of knowledge on both sides with a net result of quicker service that is more accurate and appropriate for a given situation.

7 EENA Recommendations

Stakeholders	Actions
European Authorities	Should create the necessary legal instruments to mandate the direct access to 112 by private networks and enforce them accordingly with Member States. Location information should also be made available in the same manner as regular PSTN originating calls. Competent Authorities along with the relevant stakeholders should also carry out a comprehensive study and gather data on the volumes of emergency calls from private networks.
National Government	Member States should ensure the transposition of any such legal instruments and ensure that the competent authority enforces such legal requirements in full. This should include all the relevant businesses who sell or utilise PBX equipment.
Emergency Services	The Emergency Services should ensure that their staff are suitably skilled to manage such calls and be aware of any technological developments.
National telecommunication regulators	Regulators and or the competent authorities should set the licence conditions on the relevant network providers to ensure their compliance with the direct access and location information obligations.
Telecommunication	Telecommunication Network Providers should ensure that they comply with all

[3]See also Chapter 8 of the Next Generation 112 Long Term Definition document, v1.1.

Network Providers	necessary obligations.
PBX Vendors and Users	All vendors and Users of PBX equipment need to ensure that the general public who uses the equipment must be able to connect with the emergency services without needing any trunk code. This also applies to employers whose employees use the equipment and to whom a duty of care applies. In addition, on-site notification to alert building staff that an emergency call has been placed and a visual display to assist and direct the emergency services when they arrive should be established.

A. ANNEX - US Legislative Actions

a. Suffolk County, NY

Legislator Robert Trotta had attended the NENA 9-1-1 Goes to Washington event, and met with Commissioner Pai. He took back with him, a copy of draft legislation with the intent of introducing this at the next Suffolk County Legislative meeting. The bill was introduced, and passed unanimously with no opposition. While only effective locally, it is being brought to Albany, the State Capital, for action at the State Level.

b. State of Illinois

Illinois was one of the first states to enact legislation around a tragic death of a woman trapped on the 58th floor of a tall high rise[4]. Legislation was finally enacted in December of 1999, and went into effect in June of 2000[5]. On August 11, 2014, Senator Jennifer Bertino-Tarrant successfully introduced language in SB 33-13, which passed unanimously with nearly 100% attendance, which added in language about direct access to 9-1-1 services and legislative penalties of up to $5000.[6]

c. State of Texas Commission on State Emergency Communications (CSEC)

Members of the Texas CSEC, the home State of Hank Hunt, Kari's father, were in attendance and inspired by the words of Commissioner Pai to take action. They returned from Washington DC with renewed vigour and initiated an action to review the legislative climate in the stare as well as the impact to various businesses. After publishing a report, they held a workshop that was attended by the press, the public and 911 vendors to discuss the issues, and actions forward[7].

d. State of Maryland

Delegate Joseline Peña-Melnyk introduced House Bill 1080 in conjunction with Senate Bill XXX. After reading about the incident testing direct access 9-1-1 in their own office, they were shocked to find in the Maryland House of Delegates that the MLTS failed to connect callers to the PSAP. The NENA Discussion Draft was used as the base framework to create Kari's Law that is expected to be placed on the docket during the next session.

B. US Examples

The US has not been free and clear of problems with E911 access and private networks. Most recently, Kari Hunt was murdered in a hotel room on December 1, 2013. She was attacked by her estranged husband, and although her child, only 9 years old at the time, new enough to dial 911, the hotel room they were staying in did not offer direct dial to 911. This promoted the creation and adoption of what is commonly known as "Kari's Law."

a. Kari's Law

On December 1, 2013, a tragic incident occurred in the State of Texas where a 31 year old mother was murdered by her estranged husband. Her 9-year old daughter knew the number to call was 9-1-1, however the Multi Line Telephone System (MLTS) required a 9 for an access code to reach any outside number. This prompted a response by MLTS manufacturers and State regulators to address this issue under what is known as 'Kari's Law'. The primary construct behind Kari's Law, consists of 3 primary points that have been accepted as the minimal standard for MLTS functionality. They are typically included on most MLTS systems as features that can be activated at little or no cost, and do not impose any negative impact on public safety networks. EU Policy and Regulators are encouraged to require these capabilities within the legislative frameworks surrounding all large or multi-story MLTS system installations.

[4] Chicago Tribune article, http://articles.chicagotribune.com/1987-06-05/news/8702110441_1_fatal-high-rise-fire-chicago-fire-department-fire-of-undetermined-origin
[5] Link to Illinois MLTS Legislation, as found on 9-1-1 ETC , http://911etc.com/assets/files/legisdocs/Illinois.pdf
[6] Avaya CONNECTED Blog – Interview with Senator Bertino - http://www.avaya.com/blogs/archives/2014/06/exclusive-interview-with-illinois-sen-jennifer-bertino-tarrant-on-karis-law-strengthening-911.html
[7] Texas CSEC MLTS Legislation landing page - http://www.csec.texas.gov/9-1-1/mlts#mlts-background

Unimpeded direct access (with or without any prefix, post fix or additional digits) to the designated Public Safety 9-1-1 PSAP that any public caller would reach if they were to dial the digits 9-1-1 on a PSTN telephone line.

On-Site notification, where technically feasible, to alert local building staff that a 9-1-1 call has occurred and from where. Information can be made available through a display panel in the common entrance lobby of the building in the event that there is no local staff.

MLTS Owners and Operators are specifically prohibited from impeding, intercepting, barring or joining any call in progress, unless MLTS Owner and Operator has completed the appropriate level of training and been approved by the local PSAP Director for the agency where their calls would normally terminate.

b. US Legislative Landscape (Prior to Kari's law)

At varying degrees of effectiveness and restriction, as of January 2015, only 18 States published some language within their legislation pertaining to MLTS/PBX systems. Historically these have been reactions to incidents that took place in their jurisdictions, and minimal input has been included from Public Safety, as the number of industry experts in this niche technology has been limited at best. Fortunately, there are now a larger number of experts in networking, and Voice over IP, and many have previous Public Safety exposure. Because of this, legislative language is being updated, to reflect the current market, from a technology perspective, as well as specific use cases that are applicable to those new technologies.

c. US Legislative Landscape (Post Kari's law)

After the tragic death of Kari Hunt, a Change.Org petition of 1/2 million signatures[8] led to much more awareness in the media and in the Public Safety Community. At the National Emergency Number Association 9-1-1 Goes to Washington in March 2014, FCC Commissioner Ajit Pai addressed a full room of Public Safety Officials with an initial update on an inquiry he had made to the American Hotel & Lodging Association (AHLA)[9]. In that report, he highlighted that the number of compliant hotels, including Corporate, Independent and Franchised properties, that were able to reach 911 by directly dialling 9-1-1 was "unacceptable"[10].

[8]Change.Org Petition in honor of Kari Hunt, https://www.change.org/KarisLaw
[9]Comments of FCC Commissioner Ajit Pai at 9-1-1 Goes to Washington - http://www.fcc.gov/document/commissioner-pai-remarks-9-1-1-goes-washington-conference
[10]*Id.*