



via ECFS

15 October 2014

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, DC 20554

Re: Notice of Ex Parte Presentation - Facilitating the Deployment of Text-to-911 and Other Next Generation 911 Applications, PS Docket No. 11-153; Framework for Next Generation Deployment, PS Docket No. 10-255

Dear Ms. Dortch:

MediaFriends, Inc. (dba HeyWire) is providing the following comments with regard to the Policy Statement and Third Further Notice of Proposed Rulemaking (FNPR), FCC 14-118.

MediaFriends is an interconnected OTT service provider offering IP based messaging and multi-media communications.

17. Further, the comment record indicates that technical complexities exist for interconnected text providers to deliver enhanced location. For example, Microsoft submits that, for OTT applications, “the cell site location is not readily available” and that server-based implementation approaches would require testing of location accuracy information, as well as the creation of “standardized acquisition and transmission of that location information” through TCC gateways. Bandwidth contends that there is a need for location accuracy solutions that are consistent with both established technical standards supporting existing CMRS solutions and “a broad range of application-derived location solutions commonly used by today’s OTT providers.” TCS proposes that OTT providers leverage the existing J-STD-110 standard to require that “emergency text message requests re-use existing SMS APIs in the device, effectively changing the OTT text message interaction into an SMS message dialogue . . .” TCS submits that, although this approach “would require OTT text application software modifications,” it “represents the shortest path to having support for emergency OTT text.” We seek comment on the different approaches described by TCS, as well as any additional proposals that would resolve the technical issues of covered text providers in delivering enhanced location information.

HeyWire agrees with TCS’ comment of re-using the existing SMS API’s within the device to fulfill the ability requested. This has the additional benefit of insulating both the ‘applications’ from the underlying CMRS network & technology and vice versa, thus



enabling changes & evolution without interference to the other since the OS (device) API's provide the function of an abstraction layer.

21. Similarly, we seek comment on the provision of enhanced location information with MMS-to-911 texts and for location determination of MMS callers. For purposes of providing enhanced location information, MMS-to-911 will need to be evaluated once ATIS develops such standard in which cost effectiveness of MMS is considered, as well as potential problems with receiving MMS at PSAPs. What is the status of standards work on MMS messaging to include enhanced location information? We also seek comment on what factors exist that could affect covered text providers' use of MMS to route texts to 911 with enhanced location information. Will the eventual sunset of SMS further our goal of providing dispatchable address information for communications to 911 on all text-capable media? We seek comment on the costs for covered text providers to develop, test, and implement the capability to provide enhanced location information using MMS.

The method by which the FCC has proposed for SMS implementation where by using access of the mobile device API for passing through SMS message requests for 911 services, being used for MMS will also work as long as the mobile OS environments from Apple, Google and Microsoft, that enable such, remain in place and is not blocked or disabled by the native CMRS carrier of the mobile device or any other entity with the capability or authority to effect such.

Thus, the use of the API for passing/initiating an MMS with the user's native mobile device MMS capabilities is constrained by the abilities & limits of the API.

This includes the issue of location information encompassed/associated with any MMS message regardless outside of the native CMRS carrier client. I.e. – if the API and its current abilities are curtailed, constrained or eliminated completely, regardless of source or cause of such action, it would or could have significant impacts on the ability of non-CMRS applications to implement the commission's desired use of MMS, and associated location information within those messages.

To provide an example, even if a mobile device were equipped to provide location information (e.g. – GPS, WiFi or some other method) that was available to software executing on the mobile device, if any of the elements in the 'food chain' of interdependent elements fail, the entire function will fail. If location information is not made available, if the API is altered in ways that curtail or constrained, or other functions hindered, the end goal will not be achieved of delivering MMS with location information.

It should also be noted that MMS is a much more complicated message format that can involve an incredibly diverse set of codecs, including proprietary versions, that make simple transactions such as sending a picture, possibly fail due to lack of proper transcoding capabilities or proper codec interpretation on the receiving node (e.g. -



PSAP).

An example that happens every day, a mobile user takes a picture with their device, that happens to be set to utilize some proprietary format (unbeknownst to the user) and sends the picture via an MMS message to their friend, whose mobile device does not recognize the proprietary format of the picture, and only sees a 'black screen'.

With regard to the question of whether the eventual sunset of SMS will further the commission's goal of providing dispatchable address information in communications to 911 from text capable media: this is not a binary question. A lot of variables would depend on what capabilities and parameters would encompass its replacement.

While this may seem obvious, some organization or body must set a technical format standard that the PSAP's can accept and process as the basis, and then all of the entities in the food chain on back can work from there.

Alternatively, the basis can be set at the other end of the food chain (origination) or anywhere in the middle, but, the key point is that there must be an agreed upon format and specification in order for common use to work.

It should be noted that while the use of MMS would provide significantly greater capabilities for additional data/information as well as additional functions for the purposes discussed here with FCC-14-118A1, at the current time, the majority of the CMRS providers will not interoperate with non-CMRS providers for such messaging traffic or is imposing overly restrictive (e.g. – financial terms) or selective application of conditions and terms that are only applied to non-CMRS providers.

22. Finally, the record reflects that the technological developments and standards setting efforts on LTE networks, MMS, and multimedia message emergency services (MMES) have already commenced. With developments in the CMRS wireless industry to migrate to LTE networks already underway, and the continued evolution and growth of OTT text applications in response to consumer demand, we believe that a reasonable basis exists to anticipate that within the near future, standards bodies will be adopting or releasing standards that address the provision of enhanced location information for 911 text messages. We seek comment on this view.

The question on whether within the near future, standards bodies will be adopting or replacing standards that address the provision of enhanced location information (for 911 text messages or anything else) is overly optimistic in our opinion.

While there are organizations such as the GSMA, CTIA, ATIS, etc. that are and have historically provided such direction or even provided a set reference specification for X



or Y or Z, this situation is further complicated for several reasons:

- referring to the 7-Layer OSI stack model, the function of LTE is at Layer 1 and 2 primarily (some Layer 3), whereas
- transport of messages is a Layer 3 & 4 issue
- application connection attributes are a Layer 5 issue (session control)
- messaging itself is a Layer 7 issue (application itself)

It will be difficult for any one organization to address this issue of section paragraph 95 since the typical areas of interest and *expertise* of many of the mentioned organizations typically focus on certain layers of the OSI model, whereas this question/issue encompasses all to a certain degree.

Adding to the complexity of the situation being addressed by section paragraph 95 is the fact that OTT applications are just that, 'Over the Top', and hence, the issues of Layer 1 thru 3 are irrelevant to such providers.

While it is a positive value that there is a level of separation by OTT and non-OTT, specifically the ability for everyone in the food chain from Layer 1 thru 4 (device manufacturers, carriers, network equipment manufacturers, etc.) to operate independently and without hindrance of applications that operate at Layer 5 thru 7 (this would include potentially the CMRS operators' own future applications), there does ***not*** exist any universally accepted organization to standardize, let alone discuss, of agreement on what and how applications would become universally inter-operable.

Thus, the commission's goal of having a universally accepted format (for lack of better term), especially at the application level for interoperability is extremely challenging at this point in time as such an organization does not exist.

28. Finally, what measures can or should the Commission take to address Heywire's contention that OS providers and hardware manufacturers have been removing or disabling access to geo-location functions available to applications outside of the native pre-authorized applications? How many applications and what OS platforms have been affected by this? What coordination must occur to address the issue of privacy settings?

The restricting or removal of access to geo-location function capabilities of devices originated as a result of abuse by assorted applications using the data for purposes without the user's consent or even in violation of the user's specified wishes, which is certainly understandable why restriction of access to such capabilities and functions was undertaken.

It is our belief that no amount of 'privacy settings' as a method to determine whether or



not access to geo-location or any other possible sensitive function will work because there will always be rogue applications or overly aggressive entities seeking to leverage such data and functions for their own purposes.

At a high level, only an implementation method similar to how WEA (Wireless Emergency Alerts) was handled, where a strict protocol and authorization mechanism is utilized to allow access to the function is implemented, will be sufficient to protect individuals against unauthorized use of restricted functions of their mobile devices.

In addition, there is an issue of reliance on a user's personal settings may need to be overridden in cases of emergencies, that the user themselves may want in situations of emergencies such as attempt to contact 911 type services. E.g. – if a user has set their privacy settings to disallow all access to their mobile device's geo-location functions, but, the person is in an emergency situation that requires geo-location data, the person probably is not cognizant or sufficiently aware of a need to change their privacy settings to change the geo-location function to allow the data to be collected at the time.

This entire situation is a complex technical, legal and ethical dilemma that requires adequate forethought and an implementation plan to succeed across the industry, of a similar nature to WEA.

48. We also seek comment regarding the specific costs providers of interconnected text messaging applications may incur to resolve the technical complexities in delivering enhanced location and to meet the proposed roaming requirement. To the extent those costs may vary depending on the approaches that an interconnected text provider chooses, we seek quantitative cost information on these different approaches. Further, what other potential costs, if any, to interconnected text providers should the Commission consider? Since many interconnected text providers offer their services at no charge and they may incur significant costs to implement text-to-911, will interconnected text providers have to charge for these services, or are there other ways to obtain revenues to cover those costs? Finally, we seek comment on any additional costs or burdens that covered text providers may incur as a result of our proposed requirements.

This issue/question is conceptually speculative at this point due to the unknown data elements of the multiple options presented as well as potentially available, that it is difficult to ascertain what such costs would be except for the known element and method that exists currently of obtaining enhanced location data from the mobile device itself.

As stated earlier, virtually all smart mobile devices (phones, tablets, etc.) have geo-location capabilities from technologies such as GPS and/or combination of other technologies. That data is technically retrievable "if" permitted by the underlying OS API's. In such cases, the cost would be negligible to interconnected text messaging



applications IF the applications were permitted to have access to such functions' data.

With regard to the question of whether no-charge interconnected text providers would have to charge for these services, or obtain revenues to cover these costs, it is our opinion that introduction of a charging element in what is essentially a free service would be highly problematic on multiple fronts.

First and foremost, the tens of millions of subscribers of no-charge interconnected text messaging services signed up originally with no requirement or intent of paying for the messaging services or fees. In many cases, the users of such services are poor, disadvantaged or other similarly economically challenged individuals that the availability of no-charge messaging services provided them a viable option to participate in the mobile messaging ecosystem. To add potentially even modest fees to this demographic could eliminate their ability to continue participating in the mobile ecosystem.

The modification by interconnected text messaging applications to accommodate a billing mechanism and almost surely a payment processing clearing house or similar for dealing with credit cards, debit cards, bank account debits, etc., would add even more cost overhead to the provider that could amount to millions of dollars for the industry in new costs, that may or may not be sustainable.

With regard to other ways to obtain revenues to cover such costs, in the no-charge model, in the best case scenario, the available revenue generated is from mobile advertising, is shrinking in margin and continues to do so. It is a model that is similar to broadcast television where revenues can only grow if the market dynamics such as subscriber volumes grow or advertisers determine they want access to certain demographic subscribers.

Future Texting Services

49. Scope of text-to-911 service and requirements. In this proceeding, we believe that a forward-looking view of text messaging services, encompassing all text-capable media, is necessary to ensure continued access to emergency services as covered text providers migrate from legacy 911 networks to an all-IP environment. The limitations of SMS-based text-to-911, made clear in the record, underscore the need for further development of platform architectures and standards that can deliver enhanced location and support roaming with text-to-911. As new text messaging platforms are deployed, and to ensure that all consumers can reach 911 by sending a text message, we seek comment on our ultimate goal that text-to-911 be available on all text-capable media, regardless of the transmission method (e.g., whether texts are delivered by IP or circuit-switched networks).



We agree and concur with the commission's goal "...that text-to-911 be available on all text-capable media, regardless of the transmission method".

It is our opinion that non-interconnected text messaging services should also be required to provide and support text-to-911 functions. The population will be, if not already, confused as to why a person can send an SMS to 911 on their CMRS device with the CMRS native texting application or an interconnected text messaging application, but NOT a non-interconnected text messaging application.

Many of the more popular non-interconnected text messaging applications "look and feel" like a conventional SMS texting interface, going so far in many cases of using the subscriber's mobile phone number as their identity/userid to give the perception they are 'texting'.

As the commission has cited, there are numerous evolving technologies for geo-location determination available via IP and WiFi, which when ready, would facilitate even non-CMRS networked devices (i.e. – no cellular network access; only WiFi network access) the ability to provide and execute text-to-911 functional services.

The issue of whether the commission has authority over non-interconnected services has been raised in the industry and that is the commission's prerogative, however it is our opinion that the use of phone numbers as the subscriber identity, whether actual or perceived does not matter, as the ultimate overseer of the phone numbers themselves in every country in the world is the government of that country.

51. Location Information for Wi-Fi Enabled Devices. In the Second Report and Order, we exclude 911 text messages that come from Wi-Fi only locations from the scope of the requirements at this time. In view of the record and recent trends suggesting the growth in the use of Wi-Fi generally, we believe that the public interest warrants further exploration of the feasibility of sending 911 text messages over non-CMRS networks. For instance, CMRS providers migrating to 4G LTE networks have network traffic and engineering incentives to offload their subscriber traffic on to Wi-Fi networks that are connected to wired broadband connections, such as those provided by cable or telephone companies. The Commission's Sixteenth Mobile Wireless Competition Report observed that the large demand for wireless data by mobile users at public locations has been inducing CMRS providers to reduce congestion on their mobile wireless networks, and that the forecast for total mobile data traffic offload from CMRS mobile wireless networks to wireless local area networks (WLANs), which primarily use Wi-Fi technology will increase from 11 percent (72 petabytes/month) in 2011 to 22 percent (3.1 exabytes/month) in 2016.

The issue and scenario of network transport via WiFi and non-CMRS networks is already reality. An example is the Comcast network facilitating through its XFINITY Hotspots



program free WiFi access anywhere their subscribers are located within range and if not a Comcast customer, ability to pay for access, which provides similar effects and benefit.

Additionally, companies such as Aicent (acquired by Syniverse recently) offers a WiFi roaming access capability to any service provider, including mobile carriers, through agreements with WiFi hotspot providers such as those deployed by Comcast. What this effectively provides is a network connectivity mechanism that does not rely on the CMRS network (where the person has WiFi hotspot access).

52. We seek comment on the feasibility of sending text messages to 911 via Wi-Fi networks and on the ability of covered text providers to route those texts to the proper PSAP and provide granular location data. Public safety commenters support moving ahead on evaluating location solutions that could route text-to-911 messages using Wi-Fi networks only. NENA suggests that the Commission’s medium- to long-term focus on text-to-911 should take a general approach that would address “emerging technologies such as WiFi positioning.”

With regard to this issue, it is certainly technically possible to route text-to-911 via WiFi since WiFi is only an network access technology similar to a CMRS RAN or even a wired LAN/WAN. The issue is whether sufficient data can be provided outside of the SMS text message content to properly determine its authenticity (security and integrity of the system & network is a major concern here), geo-location data, and of course sufficient ‘routing’ data to direct it to the appropriate PSAP.

All of this would be required to be determined outside of the core SMS text as the individual originating such an SMS message for 911 services will not be able to, nor should they be relied upon to do so, to provide such data.

WiFi positioning does technically work. However, the integrity of the data provided is dependent upon the integrity of the system that could be quite susceptible to changes.

It is our opinion that this is a technology that does work and can be used, but, the challenge is operational integrity and procedural processes that must be in place in order for reliability to be achieved.

53. The record includes contrasting views. For example, Heywire submits that the technical issues will require “substantial development” to address matters ranging from “the mobile devices themselves” to the “validity of the identification” of individuals who use text-to-911 on Wi-Fi only devices. Similarly, VON Coalition contends that “[i]n a Wi-Fi-only environment there is a lack of reliable location information and no reliable way for the text to be routed.” In contrast, TCS submits that “[a]dvances in the user plane protocol enable” location



techniques, including Wi-Fi and Bluetooth, that are not dependent on the macro cellular network. Also, Bandwidth describes two options for location capability with text-to-911 through Wi-Fi service: (1) “platform-derived location options,” querying a database of Wi-Fi hotspots, and knowing the Wi-Fi router locations; and (2) “off-platform services,” available to application developers ... that use hybrid positioning technology to determine a consumer’s location. We seek comment on the approaches suggested by TCS and Bandwidth, as well as any other potential solutions.

The use of WiFi technology is not the issue. The issue is the integrity (“can you trust the data”) of the WiFi system.

What happens when a WiFi hotspot is physically moved? Replaced? Upgraded? Are all the appropriate processes in place to update *all* the appropriate data sources that provide the relevant data to devices that would depend on such?

What happens if the WiFi hotspot is hacked? What if it’s hacked with malicious intent to purposely provide misleading location data to redirect first responders? Are there sufficient redundancies to provide verification in such cases?

54. Non-interconnected text applications. Additionally, the Second Further Notice sought comment on non-interconnected text applications that only support communications between a defined set of users, but do not support general communication with all or substantially all North American Numbering Plan numbers. The record shows support for addressing consumer expectations with respect to the use of such non-interconnected text applications. For instance, TCS submits that an interconnected text provider that offers a service that sends and receives text messages “between essentially any data-capable device should be required to fulfill the same 9-1-1 obligations as an OTT provider that provides such a service via one interface.” Heywire observes that the differences between an interconnected versus noninterconnected application are not understood by the average person, and that further confusion arises with non-interconnected text providers using the consumer’s mobile phone number for identification purposes or “sending an ‘authorization’ SMS message” to the consumer’s mobile device. We seek comment on the appropriate approach to address non-interconnected text services – whether through voluntary commitments or by extending the text-to-911 rules we adopt today. We also seek comment generally on the scope of non-interconnected text applications that should be covered by any requirements. Should text-to-911 requirements address non-interconnected text providers offering services to consumers who participate in social media or choose to use applications that enable texting within an affinity group but that do not use NANP numbers? What could the Commission do to encourage rather than require relevant stakeholders to implement the text platforms and technologies necessary to



achieve text to-911, and in what timeframe? What standards are being developed or would have to be adopted to allow stakeholders to implement text-to-911 on all text-capable media on a technologically neutral basis?

It is our opinion that non-interconnected text services should also be compelled to provide text-to-911 service for one overarching reason:

- the general public is *NOT* aware or can differentiate between an interconnected versus a non-interconnected text service

Many of the more popular non-interconnected text services have employed use of phone numbers, whether the mobile device's own assigned phone number from the CMRS network that the device is assigned –or- a phone number provided by the user themselves (their personal fixed line, business fixed line, personal mobile or a virtual number similar to those offered by Google Voice), to provide a pseudo 'identity' and perception that one is using a phone number and texting in the telecom sense, when in reality, they are not.

This perception of 'texting' by many non-interconnected text providers is further perpetuated by aggressive marketing messages and literature/documentation for their services of providing "texting", giving the average person the belief they are texting, and in some apps' cases, even limiting the length of the message content to 160 characters identical to SMS text messages.

It is technically possible for non-interconnected text providers to implement the same method described by the commission to utilize the OS API's for sending text-to-911 messages via the CMRS native messaging app. The OS API's are readily available to any app that is authorized by Apple, Google and Microsoft on their respective device platforms.

Assuming the commission's goal to improve public safety, would it not also be in society's interests to reduce the possible confusion on what devices and services text-to-911 is available versus asking the average person to be cognizant of such mundane issues of what is an interconnected versus non-interconnected versus CMRS provider?

55. We also seek comment on what bases of authority the Commission has that are sufficient for us to extend the scope of our text-to-911 requirements. VON Coalition opposes regulations that would apply to non-interconnected text services, especially services that "only permit users to text other users of the same service." Additionally, the Second Further Notice sought comment on non-interconnected applications that only support communications between



a defined set of users, but do not support general communication with using North American Numbering Plan numbers. The record shows support for addressing consumer expectations with respect to the use of such non-interconnected text applications. ITIC contends that this proceeding should not include text applications that “only allow consumers to communication with other users running the same application.” We seek comment on whether the legal authority set forth in the Second Report and Order would also support extending text-to-911 obligations to non-interconnected text providers. Alternatively, does the Commission have adequate bases of authority to require non-interconnected text providers to provide a bounceback message that text-to-911 service to 911 not available? VON Coalition suggests that the Commission should recommend that non-interconnected text providers “notify customers in their terms of use that texting 911 is not available” but refrain from imposing requirements on such providers. We seek comment on VON Coalition’s view.

We have no comment regarding the authority of the commission with regard to regulation in this area. Rather, it is our opinion that it is important as stated previously, that the confusion *already* in the market amongst the general public as to CMRS versus interconnected versus non-interconnected text providers will ultimately hurt consumers and the larger public safety goal of the effort if not addressed.

Stating terms and conditions in legal agreements of applications and devices, while correct and applicable in a court of law, does little in reality as the average person does NOT read them.

56. We also seek comment on the technical feasibility for non-interconnected text messaging providers to deliver texts-to-911. Bandwidth asserts that because the “application-centric model” posed in the Second Further Notice “does not depend on the 10-digit number assigned to the underlying communications device,” that model would “technically allow for the possible expansion of text-to-911 requirements to include non-interconnected OTT application providers in the future.” Heywire suggests that the CMRS-based model would be feasible for non-interconnected text providers as well as interconnected text providers. We seek comment on these proposals. What costs would non-interconnected text providers incur to comply with requirements to provide either text-to-911 or a bounce-back message?

It is our opinion that implementation of what was stated in *Second Further Notice* by ourselves and Bandwidth is minimally cost insignificant based upon our own implementation experience with non-interconnected text services ourselves.

57. Rich media text services. We also seek comment on the delivery of multimedia messages to PSAPs.⁴ Both MMS and MMES provide the capability to send multimedia,



including photos and videos, in addition to text. We seek comment on PSAP implementation of multimedia messaging services and how the delivery of multimedia could affect PSAPs. Are PSAPs concerned regarding the amount of multimedia information they may receive? Currently, certain covered text providers remove non-text content and non-911 addresses from a MMS before delivery to the PSAP. Verizon adds that the “potential for PSAP and consumer confusion” can arise “in various scenarios associated with MMS,” and that the Commission should “allow industry and public safety stakeholders to address issues concerning non-voice and non-text content in the context of NG911 systems and IP-enabled originating networks.” Verizon contends that if the Commission intends to regulate messages delivered as MMS, it will need to provide “the opportunity to resolve the technical issues in a consistent, standard way, and to address the potential for consumer confusion.” ATIS urges that “industry begin its technical evaluation quickly,” because users today connect to CMRS and Wi-Fi networks “at the same time to run SMS-like applications,” including “sophisticated applications that incorporate texting with other multimedia capabilities.” We seek comment on these industry views. We also seek comment on what factors public safety entities must consider before they can efficiently handle text, photos, and video from whatever multimedia technologies covered text and other service providers choose to deploy. What best practices are being developed as more PSAPs implement IP-based or NG911 capabilities? Do regional or virtual PSAPs provide efficiencies to filter the flow of multimedia messages to 911, especially in disasters or other critical circumstances? Should the Commission impose requirements on covered text providers to restrict multimedia information to PSAPs? What cybersecurity concerns might multimedia messages introduce for covered text providers and PSAPs? We seek comment generally on the promise and potential of media-rich text messaging services, and how soon those capabilities will be realized.

The issue of rich media services is a complex topic.

The concern regarding cybersecurity is valid since rich media enables data beyond the simple basic character set and increase in message size beyond 160-character payload, enabling potential executable code. However, the cybersecurity threat is also present with plain text messages composed of simple basic characters. E.g. – DDOS attack using simple basic character content messages.

The previous comments regarding rich media from various commenters are understandable but there will never be a 100% resolution to all the issues raised. To wait for such is futile and deprivation of the benefits of enabling PSAP’s and first responders to have potentially valuable additional data/information to assist in the 911 emergency could literally mean the difference of life-or-death.

E.g. – a person requesting 911 services may be able to assist the PSAP or first responder with pictures of their location, the incident itself or even convey the severity of the situation

With regard to the question of how soon such capabilities would be realized, in reference to previous comment regarding MMS, at the current time, the majority of the CMRS



providers will not interoperate with non-CMRS providers for such messaging traffic or is imposing overly restrictive (e.g. – financial terms) or selective application of conditions and terms that are only applied to non-CMRS providers, making an industry implementation of such services challenging at best, implausible at worst.

58. Real-Time Text. Further, we seek comment on the delivery of real-time text communications to PSAPs, wherein the text is transmitted as it is typed. The EAAC recommended that “standards and functional requirements be adopted that are technically and economically feasible” to achieve direct access to 911 using, among other IP-based text communications, real-time text communications. We note that real-time text differs from traditional forms of text communications such as SMS, in that it provides an instantaneous exchange, character by character or word by word, whereas SMS and other traditional forms of text communications require users to finish their typed message before sending it. According to the Rehabilitation Engineering Research Center for Telecommunications Access (RERC-TA), in an emergency, real-time text can allow for interruption and reduce the risk of crossed messages because the PSAP call taker is able to read the caller’s message as it is being typed, rather than waiting until the caller presses the “send” key.

Implementation of Real-time Text is technologically possible and has been implemented as early as the 1960’s in some form on networks. The issues will be the financial costs of such capabilities on every entity from the mobile devices to the networks to the PSAP termination points.

MediaFriends implemented an SMS911 bounce back function in 2012 as part of a larger effort to support SMS911 in its architecture in preparation of market desires for SMS911 services based on a ‘cloud’ product architecture to facilitate the greatest flexibility for future enhancements. The architectural underpinnings positions MediaFriends to efficiently and expeditiously conform to directives regarding SMS 911 requirements and serves the public interest.

MediaFriends Inc. has devoted enormous intellectual capital, financial resources and industry education into development of its technology and resultant products. It has expressed its willingness to provide additional information that would assist the FCC in this regard.

Pursuant to the Commission’s rules, this notice is being filed for inclusion in the public record.

Regards,

Gene Lew
Chief Technology Officer for MediaFriends, Inc., dba HeyWire