

5 December 2015

Comments of Art Botterell in re PS Docket 15-91

Wireless Emergency Alerts

The following are personal comments offered on the basis on my experience as the former manager and operational director of an integrated public warning system in a major metropolitan area, as a system architect and consultant on public warning systems internationally, as a member of the CMSAAC, and as the original designer and proponent of the Common Alerting Protocol (CAP).

Expansion of the WEA message payload

Personally I support the expansion of the WEA message payload. Since the beginning of WEA there has been concern about the challenge of writing effective 90-character alert messages. How substantial or significant that limitation actually is remains largely a topic for speculation; little empirical evidence seems to be available. However, given the strong support of potential alert originators for the expansion and the rapid advance of wireless technology and capacity, it seems appropriate and feasible to give emergency responders the option of writing somewhat longer, although still quite concise, alert messages.

Coexistence of 90 and 360 character message lengths

Any addition to the complexity of authoring WEA alerts, or any heightening of originator's fears about getting alerts right, is undesirable. The inhibiting force of "alerting anxiety" among responsible alert originators should not be underestimated. None of the options for dual-message generation suggested in the NPRM strike me as something I would want to have to explain to a police officer or firefighter under the stress and time pressure of an actual alerting situation.

However, another approach was discussed among members of the CMSAAC as a way to streamline the 90-character process. Although it was not adopted at that time, it might be worth reconsidering now that we seek a simple way to fill the 90 - character "hole" for those carriers who cannot handle full-length WEA messages.

The idea was automatically to construct a message string based on certain enumerated values within the Common Alerting Protocol (CAP) message. In particular a concatenation of values from the <source>,<event>,<responseType>,<severity>,<urgency>,<effective> and <expires> fields in a CAP message might yield a terse message like "NWS TORNADO WARNING SHELTER IN

PLACE NOW UNTIL 12:30PM". Not perfect, perhaps, but not bad either, especially if it avoids complicating the alert-authoring process. The WEA Gateway could implement this feature, once and for all users.

“Emergency Government Information” and Imminent Threat

I cannot recommend the proposed additional message category.

The category of “imminent threat” was created by the CMSAAC, not as an arbitrary label, but as a concise way of bounding the appropriate use of WEA. A misunderstanding seems to have arisen in some quarters that the “imminent threat” category is not available to local emergency managers or public safety officers. This perhaps indicates a shortfall in user education.

Under current rules both example use-cases cited in the NPRM (“boil water” advisories and shelter location information) would be appropriate topics for WEA Imminent Threat alerts from local officials, so long as there was an actual emergency ongoing or impending (i.e., an imminent threat to life or health from water contamination or from some weather phenomenon.)

What is excluded by the current category is not “emergency government information” but rather, non-emergency communications that might be construed, depending on the speaker’s viewpoint, as “education,” “advertising,” or even as political rhetoric.

WEA is a powerful communication tool, and the members of the CMSAAC were keenly aware of the need for a simple rule-of-thumb that would guard against excessive or inappropriate use of this capability. Practical experience has shown that maintaining a standard of “imminent threat to life or health” (some would append “or property”) is effective in ensuring that Wireless Emergency Alerts don’t degenerate into some other sort of platform.

(I would note further that “imminent threat” is not defined by the CAP urgency, severity and certainty values. The reverse is actually the case. A conventional table of correspondences to those technical artifacts was constructed post-facto but that did not address the crucial role of the “imminent threat” rubric as a boundary of appropriate use of WEA.)

Enhanced Content in WEA Alerts

The CAP data format permits the inclusion of URLs, phone numbers and also “binary” data objects such as digitized photos in the alert payload, but the designers recognized that not every alerting system would be capable of distributing and presenting every possible component of a CAP alert.

Photos have been intrinsic to the AMBER program since it’s inception, and NWS has pointed out the value of maps and other visualizations in maximizing public

understanding of and response to alerts. The question at this point appears to be not whether additional information resources would be beneficial, but rather, which means of delivering such information would be least demanding on the technical infrastructure.

The presentation of “rich” content such as images or other media files was obviously precluded by the original 90-character limitation on the WEA payload. However, it may be worth considering whether the one-time broadcast of, for example, a photo of a missing child as part of an enhanced WEA alert might have less negative impact on network capacity (particularly in switched networks) than the provision of a URL and the subsequent retrieval of that same information by many thousands of individuals over a short period of time.

(I would add, as an aside, that it is not necessarily a good thing to “minimize ‘milling’ behavior” as suggested in the NPRM. Milling is a critical and necessary step in the process by which audiences process and evaluate an alert; inhibiting that process will only decrease warning effectiveness. Better goals might be to facilitate or streamline the “milling” process. Fortunately social media already serve as an important adjunct to public warning systems in just that way.)

Another aspect of the URL debate is the recurrent idea of recipient feedback or acknowledgement of alerts. But when alerting an audience of thousands, tens of thousands or more, it becomes debatable whether responses are actually helpful.

I am aware of no evidence that people who acknowledge that they’ve received an alert are necessarily more motivated to take appropriate protective action, which is the practical goal of emergency alerts. Much more significant are real-world metrics of actual public behavior, for example, freeway traffic statistics during an evacuation.

Neither is it clear what useable information could be extracted from a massive stream of acknowledgement messages, nor what expectations the provision of an individual response mechanism might raise in members of the public. Nothing in the WARN Act suggests that WEA was ever intended to impinge on the role of Next Generation 9-1-1.

Providing Multilingual WEA Messages

CAP provided for multilingual alerting from the start. What we soon discovered was that the real challenge wasn’t so much one of disseminating multilingual alerts as it was of authorities’ generating them in the first place. Most public safety officers and emergency managers have very limited capacity, if any, to generate timely translations of specific alerting messages into multiple languages.

This is a challenge that has been faced by authorities in Canada and also in a number of Caribbean nations. No really satisfactory solution has yet been found. If forced to generate multilingual alerts, most originators have taken refuge in using pre-scripted alert texts that sacrifice specificity and flexibility in pursuit of multilingualism.

Still, there is no reason the technology of WEA should inhibit dissemination of alerts in languages other than English when they are available. The CAP format used at the input to the IPAWS already supports full internationalization. However the industry-specific protocol used at the IPAWS “C” Interface (between FEMA’s servers and the wireless carriers) may require some revision.

Enhancing WEA Geo-Targeting

The goal of geo-targeting alerts is to maximize the relevance of received alerts, minimizing both the Type I error of “over delivery” and the Type II error of “missed recipients.” Typically alert originators get fewer complaints from people who received an alert that was at least potentially relevant to them than from people who received an alert that certainly wasn’t.

During the Cold War era it chanced that the extent of a thermonuclear weapon’s effects was roughly on the order of the size of a typical county. The county became the default “granularity” for targeting alerts in the era of CONELRAD and EBS and even in today’s EAS. But the vast majority of today’s threats are much more limited in area. It is not uncommon, especially in urban areas, for local officials need to target an alert to an area as small as a few city blocks.

A county, even in the Eastern US where counties tend to be smaller in extent, encompasses much too large an area for the vast majority of warning scenarios. The inherent “over warning” or “spill” of county-level geo-targeting often makes use of WEA (and EAS) politically infeasible for tactical-level responders who fear to risk large-scale public criticism.

Meanwhile, from the alert recipient’s perspective, that individual may be concerned with events affecting locations other than her or his current position. For example, an alert affecting a child’s school, or a business location, or, for a traveler, her or his home may also be of great interest. A system that can only route messages to people whose current location lies in the target area do not address the “location of interest”

This brings us to the question of “device-based solutions.” By providing the actual bounds of the CAP alert area to a location-aware end device, we could make it possible for modern “location aware” smartphones to determine not only whether that device is in the target area, but also if any user-designated location of interest is affected. At a stroke we remove many of the complexities and costs of limiting transmission precisely by selecting cell sites or sectors.

This leveraging of smartphones and other location-aware receiving devices was a key use-case in the design of the Common Alerting Protocol. While it is not the only way of approaching geo-targeting in WEA, it still has much to recommend it.

WEA Testing and Proficiency Training

In my view the opt-in approach for receiving test alerts best meets the needs of public safety users. A key goal of user training on any alerting system is to provide assurance that nothing bad will happen to the officer or official who uses the system appropriately. That is best demonstrated, and success in the technical aspects of training best evaluated, by actually allowing the trainee to perform a complete test activation. As long as anyone with an interest can choose to receive the test alerts, there is no particular benefit in exposing such messages on the general public.

Note that in a class setting, which is where such training is typically done, having each student perform a test activation will result in a “burst” of test traffic typically within an interval of an hour or less. While it is not clear that there is a need to limit the amount of test traffic on the WEA system, such limits if deemed necessary should not be cast in terms of long-term periodicity, but should recognize and accommodate the “bursty” nature of training traffic.

The 24-hour delivery window for RMTs certainly should not be extended to State/Local WEA tests and should be re-evaluated for RMTs. Nothing will undermine new adopters’ confidence in WEA more than sending off test alerts and seeing no result in a reasonable time period for urgent alerts. From the originators’ perspective a 24-hour delay of an alert, even if just for testing or training, is as bad or worse than no delivery at all.

Non-commercial Educational and Public Broadcast Television Stations

Prior to the passage of the WARN Act I was involved in successful FEMA tests of a Digital EAS utilizing educational television signals in the Washington, D.C. area. Those experiments were highly influential in the development of the Common Alerting Protocol.

Non-Commercial Educational (NCE) TV stations’ “datacast” of alerts, particularly to location-aware receivers, have great potential for providing an “always on” public awareness stream without the degree of intrusiveness associated with WEA. Given their considerable power and bandwidth, the digital transmitters of NCE stations can provide the sort of rich information that WEA currently struggles to deliver. Alerts transmitted by this means could serve as an input to further CAP-compliant alert dissemination and display systems, e.g., public digital signage, and for triggering of sirens and other alerting systems.

I would strongly recommend that the NCE datacasts NOT be treated as an extension of the WEA “C” interface, which uses a wireless-industry-specific data format that strips out much of the potential richness of the CAP format. Instead, NCE datacasts should utilize the CAP formatted data provided by the originator to ensure maximum compatibility with “downstream” systems. Indeed, it would not be unfeasible to stream the entire corpus of current IPAWS alerts, complete with “rich media” attachments, as a continuous “carrousel” data service over NCE transmitters.

In Closing

Applause is due the Commission for its perseverance in revisiting a number of important questions that were left open for future review by the CMSAAC, and for taking a forward-looking approach to the WEA rules. I hope and trust the Commission will also not consider this current proceeding an end-point. Technology will continue to evolve, as will our social and threat environments. Our public safety and security systems will need to be reviewed and updated regularly.

Respectfully,

ART BOTTERELL

3400 Nantucket Drive
Fairfield, CA 94534
(707) 750-1006
art@botterell.net