ONE2MANY
AN EVERBRIDGE COMPANY

TECHNOLOGY COMPARISON FOR NATIONWIDE PUBLIC WARNING SOLUTIONS

A guide to help you compare and assess the most effective technology for nationwide public warning alerts. Making sure that you're prepared for the unexpected.

When it comes to nationwide public warning, effective communication is at the heart of multi-hazard alerting systems; before, during, and after an emergency. Being able to get the right message, to the right people, at the right time – quickly, all depends on the technology you select.

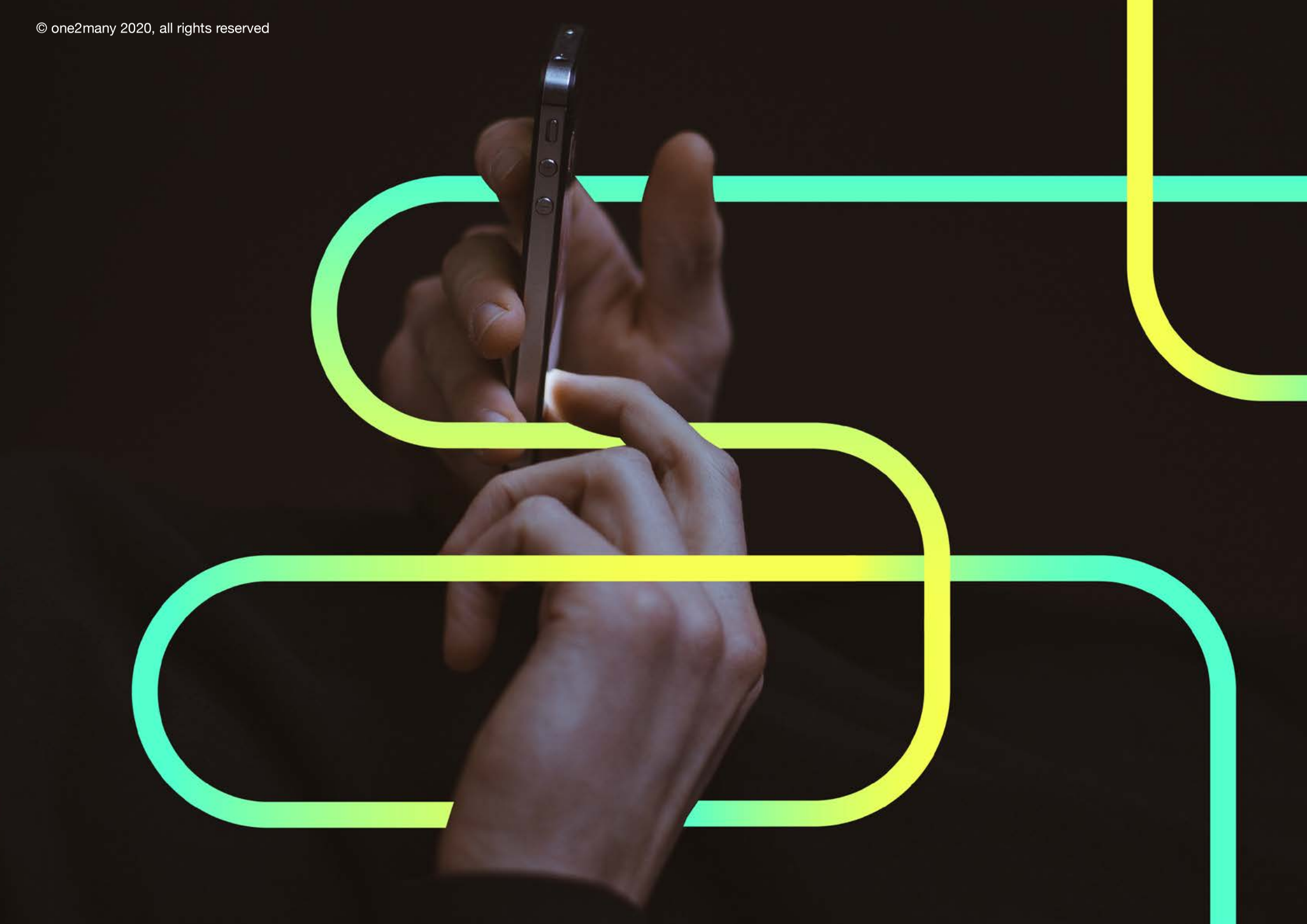
INTRODUCTION

Emergency alerts are an essential element of providing for nationwide public safety. Studies have shown that having an effective Public Warning Solution (PWS) substantially reduces deaths, injuries, and damage. The alerts need to reach all those in the affected area(s) as fast as the emergency dictates. Clear messages from a trusted source, that provide instructions and advice for residents, visitors as well as the emergency management teams to help safeguard lives and livelihoods.

Yet, nationwide public warning is about more than setting policy. It's choosing the right underlying technology service that supports your countrywide operating practices, allowing you to enforce jurisdiction while applying approval and notification rules. As well as meeting the criteria of the various emergency warning requirements, be it EU-Alert, W-PAS, KPAS, ETWS, EMA, CMAS, WEA, to name a few.

Given the extensive reach of mobile networks, leveraging the ever-present mobile device to send life-saving information to citizens is a natural choice for the primary channel. Arguably though, all PWS must be multi-channel so you can disseminate supplementary information. For instance, posting a social media alert, creating an RSS feed, sending an email, or updating electronic signage. Leveraging the benefits of each communication channel, you amplify the call for action by providing corroborating information. However, the key decision to be made when implementing a PWS is selecting the most effective primary alerting channel. The channel you rely on to get the right message, to the right people, at the right time – quickly!

This guide is designed to help you compare the three leading PWS technologies: cell broadcast, location-based SMS, and app-based solutions. There is a section for each technology that provides a general description of the pros and cons. To wrap up, there's an 'at-a-glance' comparison table for a quick reference summary.



WIRELESS EMERGENCY ALERT REQUIREMENTS

While there are some country-specific adaptions in the various wireless emergency alert requirements, when it comes to the essential ones, there are commonalities across them all. They can be summarized as follows:

- Reach the maximum of a population,
- 'No download/sign-up', including visitors
- Location specific information to be received during a crisis in specific areas
- Fast delivery. Timing is everything.
- Should always work, even if the mobile network is congested or network access is barred
- The public's privacy should not be compromised
- Only Government agencies should be able to issue alerts
- Attract the public's attention and initiate a call for action
- Adhere to international Standards
- Free to receive

It is these which form the basis of this technology comparison. Crucially, the guide helps you assess the effectiveness of the technology service when it is used as a primary channel for mobile device based wireless emergency alerts.

CELL BROADCAST

By its very nature, a cell broadcast-based PWS is a location-based service. Alerts and warning messages are sent to a specified area, reaching all those within it, whether you are a resident or visitor. With the cell broadcast service, warning messages and alerts are repeated at a pre-defined interval. Any new person entering that area will automatically receive it as the system has a unique identifier ensuring that communication is not repeatedly shown unnecessarily. But if you have already received it, the message won't be presented again.

With the enhanced ATIS standard, WEA 3.0 has introduced device-based geo-fencing. The geo-fencing feature of cell broadcast uses satellite navigation, e.g., Galileo, in addition to the cell information to establish the location of the mobile device. This allows cell broadcast messages to be more precisely delivered, with an accuracy of meters, by using the mobile device's actual location.

The cell broadcast service is supported on all devices and has been commonly available on Android, iOS, and Windows mobile devices since 2012. Although in some countries, the Government and Mobile Operators do need to inform the device manufacturers to pre-set cell broadcast alerts on mobile devices automatically. You don't need to download or register. It's free.

With the cell broadcast service being available on all mobile devices, the Dutch Government stated, in June 2020, that their regular bi-annual test alert message reached 94% of the Dutch population of 12 years and older.

Depending on the nature of the emergency, speed is critical; for instance, with a tsunami or a bomb threat. With a cell broadcast service, it only takes seconds to send a warning message to millions of people.

The purpose of sending emergency communication is to attract people's attention and guide them to safety. With a cell broadcast PWS, messages are automatically displayed. No interaction to see the message is required. Cell broadcast doesn't, however, provide a network confirmation of alert receipt. Still, as you need to acknowledge the warning message before you can continue using your mobile, it ensures that the alert is read. With cell broadcast, Governments can set up different channels for different types of alerts, with citizens having the option of which non-mandatory alerts they want to receive.

Cell-broadcast is the only emergency warning technology service that is standardized. As a result, there is a unique standardized ringtone and vibration. Only used for emergency communication. It's used across the world. It's instantly recognizable as an emergency alert, and there is no confusion as to whether it's for a regular SMS or application message.

Using the device's language settings, information contained in the emergency message is automatically received in your chosen language. With up to 1395 characters, a cell broadcast PWS enables you to provide relevant and clear instructions. All received messages are retrievable, which lets you refer back to the instructions in case you've forgotten what to do or where to go. As communication is location-specific, the messages for that area can be updated during the course of the emergency, ensuring that the latest information is provided. People receive up to date advice, related to their current location.

The cell broadcast service is part of the mobile network's signaling. Under 3GPP standards, cell broadcast by default has priority over any

other service and, in some cases, utilizes a separate channel to regular messaging traffic. The service is not affected by mobile network congestion, whether this is a crowded area such as a stadium or as a result of increased traffic due to people urgently trying to contact their loved ones during an emergency. What's more, a cell broadcast PWS doesn't contribute to network congestion. It requires only one message per cell to be sent to reach all the mobile devices within that specified area. Also, alerts and messages sent using the cell broadcast service are not impacted if the mobile network is deliberately closed to the general population to allow only emergency responder SIM class-based access. Everyone in that specified area still receives the emergency communication.

In an emergency, the public needs to be sure that any emergency alerts originate from the Government. As a cell broadcast-based technology, the PWS is as secure as the mobile network itself. With a cell broadcast PWS, only designated authorized agencies can send emergency alerts. The alert can't be forwarded or changed.

From a privacy perspective, a cell broadcast PWS sends alerts and emergency messages to all people in the specified area without needing to know their mobile number. The solution utilizes the anonymous nature of the cell broadcast technology that is effectively unaware of the recipients. With a cell broadcast PWS there is no location-based server that keeps track of a person's mobile location. People's privacy is protected. It's completely unaffected.

LOCATION-BASED SMS

SMS is, undoubtedly, a globally known technology, with most of the population being familiar with SMS text messages. As the name would suggest, location-based SMS (LB-SMS) uses the existing SMS channel, and alerts are sent to mobile devices within the emergency area, which have an active subscription (SIM card). Yet, when it comes to emergency alerting, there are two perceptions regarding location-based SMS, which need clarification.

Firstly, is the perception that it utilizes similar precision location technology to applications on the mobile device such as Google Maps' satellite navigation. This is not the case. LB-SMS relies on the mobile network for the device location. Secondly, although traditional SMS is standardized and is supported by close to 100% of all mobile phones on all networks, you need to ensure that you're assessing the technology service for emergency alerting. LB-SMS is not a standardized emergency alerting technology. LB-SMS relies on a Mobile Location Center (MLC) deployed in the mobile network. As there is no location-based SMS standardization for emergency alerting, this means that the functionality of the MLC can vary. The result is that the accuracy of the location information is very much dependent on how good the MLC is. An MLC is particularly important to ensure that roamers (visitors) are included in the alert dissemination. Also, with LB-SMS, there is a location latency to be taken into account. On average, the mobile network updates device location details approximately every 20 minutes, if there is no activity on the device in the meantime. LB-SMS is not real-time location-based.

With LB-SMS leveraging the traditional SMS channel, it is recognizable and familiar to the majority of people. There is no download required or registration, and it is free to use. The only scenario where a charge could be levied is for visitors to the emergency hit area who are roaming, for example, people on vacation or business. Depending on the country-specific roaming agreements, the alert might be charged at the standard roaming SMS rate.

LB-SMS is a one-to-one technology, which means that the PWS sends an individual SMS to each mobile device. To do so, the PWS identifies the actual list of mobile subscribers in the area. Once an alert has been issued, there is a receipt acknowledgement that it was delivered to the device. Here, a distinction needs to be made; a delivery receipt acknowledgement is not equivalent to a read receipt acknowledgement. As there is no acknowledgment required by the recipient of the alert, it cannot be guaranteed that the emergency message has been seen, but it is proof that the message reached the mobile device. The count of recipients can undoubtedly be useful when it comes to crowd management as the location-based SMS PWS can track the flow of mobile device subscribers within an area.

When it comes to the emergency message itself, as the LB-SMS PWS requires the network to deliver individual messages to each recipient, you can provide alert advice in the native language, for instance, by identifying the mobile country code from the SIM. However, this approach doesn't take into account Expats or immigrants who have a local mobile device but may not fully understand that local language. Depending on the special characters, the length of the emergency message varies up to the maximum 160 characters. This may impact the detail of advice or instructions to follow. Although it is possible to send concatenated SMS messages, some mobile devices will only display the full message when all the segments have been received. Concatenation will add extra load on the network with more messages being disseminated.

As messages from a LB-SMS PWS are sent by SMS, the ringtone and vibration of that emergency alert are the same as the other SMS which the person receives. When it comes to attracting people's attention in an emergency, this means there is no distinction between a regular and emergency message. Like all the technologies, LB-SMS can support 2-way communication should that be required as part of the crisis management working practices: be it replying to an SMS or clicking on a weblink/URL.

Despite network capacity increasing over the years, LB-SMS PWS can still be affected by network congestion. The reason for this is that the radio/spectrum of the mobile network cell becomes the bottleneck for delivering the one-to-one based message. Most cells have a limit of just 25 parallel sessions. This can result in messages taking up to 20 minutes or more to be delivered. In the worst case, it can take hours, as a study in Portugal proved. It took approximately an hour to reach 80-90% of a population of 300,000, and the reach reduced to only 40-50% for a population of 1 million. Although 3GPP has standardized prioritized SMS, in an emergency warning context, the term prioritized SMS is misleading. The prefix 'prioritized' doesn't eradicate the inherent underlying network challenges with SMS technology. If the mobile operator's network is congested, all SMS messages are impacted.

The reach of LB-SMS is also affected if the mobile network is deliberately closed or barred to the general population to allow only first responder SIM-based access.

From a privacy perspective, LB-SMS PWS relies on the mobile network to track citizens' mobile devices. Although this information is stored within the mobile operator's network, the European Electronics Communication Code (EECC) Directive, does ensure citizen privacy is not compromised. For countries that fall outside of the EECC Directive, updates to their laws may be required as privacy laws vary per country.

Given the importance of emergency alerts, the security of a PWS is critical, and the public needs reassurance that the alert comes from a trusted source. Extra vigilance is required for LB-SMS PWS. With the availability of commercial SMS Gateways on the internet that allow the user to set the source Mobile Subscriber ISDN Number combined with a tech savvy malicious person's ability to spoof SMS messages, there are additional security risks to be taken into account.

APP-BASED SOLUTIONS

With the increasing popularity and familiarization of internet-based apps across the general population, an App-based (A-B) PWS solution could be considered. Actively encouraging citizens to download the app does need to be factored in. In Germany and France, for instance, only a fraction of the population took the effort to download and use the emergency mobile app. Less than 3% of the German population and less than 1% in France.

From a location point of view, an A-B PWS can leverage the latest combination of technology (e.g., GPS, satellite navigation, WiFi) to accurately pinpoint the mobile device within meters, if the person has granted permission to the emergency app to use the mobile device location.

From an emergency message perspective, when using A-B PWS, you are not restricted to only text, and there is no fixed limit to the message length. The A-B PWS can be configured to send alerts in multiple languages by mirroring the mobile device's language settings. Any mobile device within the coverage of the A-B PWS location service will receive the alert and any updates. This includes visitors as well as people who may have entered the emergency area after the initial message was disseminated. Generally, mobile network operators charge for internet access. Unless a zero-rated mechanism is deployed, there may be a cost associated with receiving the emergency alert. If a person has exceeded their data bundle limit or has disabled data connectivity during roaming, they may not even receive the alert.

It is possible to define a separate ringtone and vibration for emergency messages. Although, it is important to highlight, each A-B PWS needs to be examined on its own merits as it is not a standardized emergency alert service. Functionality and effectiveness can vary. There is no global standard for implementing A-B PWS.

Unlike cell broadcast and LB-SMS, there is more reliance on, and participation required from the general population for an A-B PWS. The emergency application must be downloaded, with regular updates installed. From a reach perspective, on-device applications are typically designed for Android and iOS smartphones using at least a 3G network. As such, apps are not supported on 2G networks, nor on feature phones, which for some Governments remains an important consideration. Also, it is not guaranteed that the app remains on the mobile device. There is a risk that the app could be deleted should there not be sufficient storage capacity on the mobile device or that it is not re-installed when the person changes their mobile device. But, what about overseas visitors to the emergency area? How will they be informed about the app, and would they need to install a different app for each country they visit?

A-B PWS is a one-to-one service, sending individual alerts to each mobile device. And, although an A-B PWS can work without being deployed within an operator's mobile network, as it is an Over-The-Top (OTT) application, the emergency service is still affected by network data congestion. Should the data network be barred or affected, the dissemination of the alerts will be impacted. Although WiFi data spots could be used as an alternative data path, it would require an effective country wide network to provide the necessary coverage and reach.

Security for any internet-based solution requires robust IT protocols to prevent attempts by hackers to exploit the A-B PWS. Although A-B PWS uses end-to-end encryption for messages, including cryptographic signatures to verify the identity of the message originator, as a trusted Government source, and prevent against modification may increase trust levels.


ilno

TECHNOLOGY COMPARISON REFERENCE SUMMARY

DESCRIPTION	CELL BROADCAST	LOCATION-BASED SMS	APP	NOTES
Reach maximum population				
Supported in 2G, 3G, 4G, 5G mobile networks	Yes	Yes	Not 2G	
Supported in smart phones	Yes	Yes	Yes	
Supported in feature phones	Yes	Yes	No	
Download required	No	No	Yes	
Sign-up required	No	No	No*	(*) Sign-up maybe implicit when a user downloads the App from their application provider.
Multiple alert channels available	Yes	No	Yes	
Citizen acknowledges emergency alert on device	Yes	No	Yes	
Location specific information				
Location specific information	Yes	Yes	Yes	
Location accuracy	cell/meters*	cell/meters**	meters	(*) When using device-based geo-fencing capability increases this to meters (**) Requires a high functioning MLC for meters accuracy.
Location latency	None	20 mins*	None	(*) On average a mobile network updates subscriber location every 20 minute, for who is in the target area.
Continuous guidance, including updates to running alerts	Yes	Yes	Yes	
Fast delivery				
Maximum speed of alert dissemination	All citizens in 4-10 seconds	25 parallel sessions per cell*	50 parallel sessions per cell	(*) Despite large centralized data and SMS capacity, the radio/spectrum capacity of each cell is a bottleneck for delivery for the one-to-one based messages.
Always work				
Alert dissemination affected by network congestion	No	Yes	Yes	
Alert dissemination contributes to network congestion	No	Yes	Yes	
Alerts received if network barred	Yes	No	No	
Privacy not compromised				
Subscriber location required for alert dissemination	No	Yes	No	
Count and location of subscribers retrievable	No	Yes	Yes	
Change in country privacy laws required	No	Yes	No	(*) Depends on country specific laws.

DESCRIPTION	CELL BROADCAST	LOCATION-BASED SMS	APP	NOTES
Security - only Government authorized usage				
Alert can be hacked and manipulated	No	Yes*	Yes*	(*) Hackers are known to spoof SMS messages and for any internet-based application there is a cyber-attack risk.
Alert can be re-routed or intercepted	No	Yes	No	
Alert can be forwarded or changed by recipient	No	Yes	No	
Security level of alert messages	High*	Low	High**	(*) Cell broadcast uses network signaling security, encryption with direct RAN access. (**) Applications have end-to-end encryption and authentication
Call to action				
Alerts are visibly distinct from other notifications	Yes*	No	Yes	(*) Direct display on mobile screen
Alerts are audibly distinct from other notifications	Yes*	No	No	(*) Standardized specific ringtone
Alerts are tactility distinct from other notifications	Yes*	No	No	(*) Standardized specific vibration
Alerts are recognizable when travelling abroad	Yes	No	Yes	
Support for alert messages longer than 160 characters, without sending multiple messages or concatenation	Yes	No	Yes	
Support of URL or weblink in the alert messages	Yes	Yes	Yes	
Support of responding back to the alert authorities	Yes	Yes		
Receiving of an acknowledgement that the subscriber has received the alert message	No	Yes	Yes	
Receiving of acknowledgement that a Cell successfully has submitted the alert message	Yes	No	No	
Adheres to international standards				
3GPP/ETSI emergency alert standardization	Yes	No	No	
Compatible with worldwide PWS standards (e.g. CMAS, EU-Alert, KPAS, KTWS)	Yes	No	No	
Adheres to international standards				
Free for citizens to use	Yes	Yes	No*	(*) App uses mobile data (credits)
Free for roaming citizen	Yes	No	No	(*) Dependent on roaming agreements

ONE2MANY

AN EVERBRIDGE COMPANY

INFO@ONE2MANY.EU