PSCEurope
Public Safety Communication Europe

 PSCE White Paper

Getting it right first time

Implementing Article 110, European Electronic Communications Code 2018

March 2019

Contents

To complement publication of this White Paper, PSCE has organised a project initiation workshop on 16 May 2019 at the Belgian Police Headquarters, Rue Royale 202, 1000, Brussels, Belgium. To register your attendance, please visit: https://www.psc-europe.eu/

Disclaimer

The author has endeavoured to provide fair and factually accurate information about Public Warning Systems, but recognises that it is not always possible to cover every aspect of this topic. Hence, there may be some omissions.

Executive Summary

i This White Paper complements the 16 May 2019 project initiation workshop organised by Public Safety Communications Europe (PSCE) on implementing Article 110, European Electronic Communications Code (EECC), "Public Warning System". EU Member States without a compliant capability now have a duty to deliver an effective Public Warning System (PWS) by June 2022.

ii This first document on implementing Article 110 EECC explains to national project teams the importance of an outcomes-driven and requirements-led approach. The first focus must be on fulfilling the community safety outcomes, legal obligations and operational requirements in the scope and design of this life-saving system. Subsequent PSCE workshops will review available technologies against these critical success factors. They will also explore concurrent work streams for multi-State and regional collaboration.

iii Much has been written previously about Cell Broadcast (CB) as a public alerting dissemination technology that was intended, principally, for infrequent large-scale disasters. This White Paper addresses and resolves a significant failing in those predominantly technology-focused reports that said little if anything about the critical success factors for a PWS. These are that in today's omnipresent threat and risk environment, the PWS needs to be a much broader all hazards, all agencies capability, which only the Location Based SMS (LBSMS) technology can deliver, either instead of or on top of CB. Those critical success factors must take full account of:

- **Community expectations** to ensure public inclusivity/access, and operational use for both large-scale disasters and the more day-to-day, localised emergencies;
- **Operational requirements** of all the user authorities;
- **Legal obligations** to fulfil a statutory duty to warn and inform the public;
- **Community confidence** through automated system assurance, audit and accountability on a proven platform that delivers alerts every time successfully to everyone in the area affected on their choice of mobile telephone, and
- **Maximising the return on investment** through a scalable, multi-purpose platform.

iv This White Paper demonstrates how countries such as Belgium, Iceland and Australia benefit from having opened up the scope at the initial design stage to develop a much broader all hazards, all agencies capability, built on a common platform as an enterprise architecture using LBSMS. This has the ability to support the concurrent needs of:

- **Public Safety** (localised, day-to-day emergencies)
- **Disaster Management** (large-scale events), and
- **National Security** (lawful use of data for serious crime investigations).

The alternative CB platform delivers only a limited public alerting capability.

v Therefore, a key objective of this paper is to help EU Member States maximise the return on their investment in their choice of PWS platform by ensuring the scope and design take full account of the emerging and enduring needs of all its user authorities.

vi This White Paper includes a set of case studies to help illustrate the importance of taking an outcomes-driven and requirements-led approach to scoping the project correctly from the start. This avoids the sub-optimal outcomes experienced by a number of countries that include the USA, Canada, and New Zealand. They took a technology/industry/ regulator-led approach that fulfilled only a very narrow set of public alerting requirements. They now face the challenges, potentially, of retrofitting a much broader scope, for which the CB technology first chosen was not designed.

vii The alternative approach is the one advocated for in this paper that delivers the all hazards, all agencies capability that the user authorities require and the community expects, which LBSMS provides. Nevertheless, for some Member States with a national risk and threat profile involving both large-scale disasters and localised emergencies, there may be clear benefits from combining CB with LBSMS on one PWS platform.

Getting it right first time

1. Purpose

This paper is intended to inform officials (and technology suppliers) with responsibility for implementing Article 110 EECC on how to design and implement the PWS successfully to get it right first time. Many countries that did not focus their PWS projects from the start on being outcomes-driven and requirements-led now have sub-optimal systems, with only limited functionality and, thus, a narrow set of public safety benefits. Authorities may have to re-engineer, replace or add to them with an alternative technology at extra cost. This paper takes that international learning to help explain the benefits of scoping the project correctly from the outset to deliver the optimal capability and achieve the greatest value from the initial investment.

2. New EU Legal Requirement

2.1 On 11 December 2018, Article 110 EECC passed into EU law[1]. This Directive mandates that, by June 2022, every EU Member State must implement (if it has not done so already) a PWS that can reach mobile phone users affected by major emergencies and disasters.

Article 110 Public Warning System

1. *By June 2022, Member States shall ensure that, when public warning systems regarding imminent or developing major emergencies and disasters are in place, public warnings are transmitted by providers of mobile number-based interpersonal communications services to the end-users concerned.*

2. *Notwithstanding paragraph 1, Member States may determine that public warnings be transmitted through publicly available electronic communications services other than those referred to in paragraph 1, and other than broadcasting services, or through a mobile application relying on an internet access service, provided that the effectiveness of the public warning system is equivalent in terms of coverage and capacity to reach end-users, including those only temporarily present in the area concerned, taking utmost account of BEREC[2] guidelines. Public warnings shall be easy for end-users to receive.*

By June 2020 and after consulting the authorities in charge of PSAPs[3], BEREC shall publish guidelines on how to assess whether the effectiveness of public warning systems under this paragraph is equivalent to the effectiveness of those under paragraph 1.

Recital 260aa: "End-users concerned should be deemed to be those end-users who are located in the geographic areas potentially being affected by imminent or developing major emergencies and disasters during the warning period, as determined by the competent authorities".

Recital 260ab: "In the course of the future review of this Directive, the Commission could also assess whether it is possible, in accordance with Union law, and feasible to set up a single EU-wide public warning system in order to alert the public in the event of an imminent or developing disaster or major state of emergency across different Member States".

2.2 **Key points from Article 110 and Recital 260aa:**

Paragraphs 1 and 2:

(i) Mandatory implementation of a PWS by June 2022, which

(ii) Shall alert citizens and visitors alike, regardless of whether he/she is a resident or only temporarily within the area affected.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972&from=EN
[2] BEREC – Body of European Regulators for Electronic Communications.
[3] PSAPs – Public Safety Answering Points; e.g. 1-1-2 call-taking and dispatch.

Paragraph 1 only:

(i) Transmission of the alerts shall be done via the mobile public telephone networks, and

(ii) Received on the mobile telephone of choice carried by each resident, citizen and visitor.

Therefore, from day-one, **it must be accessible equally to and reach everyone with a mobile phone in the area affected, whether local residents, national citizens transiting through, or foreign visitors, regardless of their choice of service provider or mobile phone.**

Paragraph 2 only:

(i) The alternative technology shall be as effective as that used in 1, and

(ii) Utilise a publicly available electronic communications technology, which does not include TV and radio broadcasts or a smartphone application.

2.3 **Potential technology options**

Paragraph 1

(i) **Location Based SMS (LBSMS)** and/or (a blended option)

(ii) **Cell Broadcast (CB)**.

Paragraph 2: A viable alternative to (i) and (ii) above.

2.4 **Recital 260ab:** The recommendation from this provision is that Member States need to be mindful of future-proofing their preferred solution by choosing a technology or blend of technologies that allow for interoperability between Member States.

3. Capability

3.1 **The PWS provides the capability, in an emergency, for relevant authorities to communicate quickly with the public via their mobile phone when they are within the area affected by that emergency, alert them remotely to the risk, and provide the information they need to take action.**[4]

3.2 With around 92% of the EU population now owning a mobile phone (forecast to reach 1.241 billion users by 2020[5]), and given the omnipresent threat from multiple natural and man-made hazards, the PWS needs to be a universally accessible system that can reach the vast majority (ideally, more than 95%) of mobile phone users within the affected area.

4. Community Safety Benefits

4.1 In an emergency, we measure the success of the PWS by a single outcome: **That individuals, households and families have the information needed to make good and timely decisions to act[6].**

4.2 Therefore, the principal requirement for the PWS is that, in an emergency, it is: **The trusted, reliable, inclusive source of timely, authoritative, relevant and factual information about what the authorities know at that moment and what they want the public to do in response**.[7]

4.3 The primary functions of the PWS are, therefore, to provide relevant authorities with the capability remotely through the PWS platform to:

- Deliver the first and intrusive **Alert** to warn the people affected of the location and nature of the emergency;

[4] Author's definition.
[5] https://www.statista.com/statistics/218977/number-of-mobile-users-in-europe-since-2010/
[6] Author's proposition.
[7] Author's proposition.

- Tell them what **Action** they need to take in response;
- Provide critical **Updates**, such as the threat has changed direction, and
- Advise of **Closure**, when the incident is over and people can return to normality.

4.4 To avoid less optimal outcomes and, thereby, reduced benefits to community safety, EU Member States must in the initial design stage:

- Acknowledge the community's expectations of the PWS and that demand will grow (as it has done in Australia). Hence, the initial system needs to have the capacity to evolve and, thus, be scalable and future-proofed from the start, and
- Determine the operational needs and functional requirements of all their user authorities. This includes the changes required to operational procedures, policies and governing legislation to optimise use.

5. Fundamental Design Principles

5.1 The ideal outcome from each national project to design and deploy an operationally effective PWS is to deliver an all hazards, all agencies capability. This has to be delivered as a total package that combines four key elements:

1. **Community education**
2. **Operational transformation**
3. **Legislation, policy and standards**, and
4. **Technology** (choice, systems integration and rollout).

5.2 The first consideration is for relevant authorities in each Member State to assess collectively their functional and operational requirements against the National Risk and Threat Register (or equivalent)[8]. This process of mapping requirements against each risk and threat scenario will identify the:

- **Community safety outcomes expected from the system**
- **Operational and functional requirements for an all hazards, all agencies capability**
- **Accountability and system assurance**
- **Lawful access to mobile communications data**
- **Changes to legislation and the authorities' operating procedures**, and the
- **Community education and awareness programme.**

5.3 Some risks will be of imprecise, large-scale disasters that include, earthquake, tsunami, wildfires, floods and storms. EU Member States may determine that if these are the principal risks for which their authorities will use the PWS, then they may perceive the need is only for a wide-area (national or regional) capability using CB.

5.4 Experience from Australia shows, however, that the public will expect, and authorities will also want to use the PWS for the more regular threats to life and livelihoods in very precise geographical areas. These include:

- Acts of terrorism, including chemical and biological attacks
- Suspect vehicle (potential vehicle borne improvised explosive device/car bomb)
- Marauding terrorist attack – knives, explosives, firearms and vehicles
- Active shooter
- Police vehicle pursuits
- Gas leaks and the release of other toxic fumes
- Water contamination
- Structural fires, building damage and evacuations

[8] https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/theuksnationalriskassessmentnra.htm

- Crowd safety
- Major disruptions to transport networks
- Emergencies at COMAH[9] sites, and
- Vulnerable missing persons.

For these types of more localised, life-at-risk emergencies, EU Member States may determine they need a LBSMS platform that delivers a geographically precise alerting system with automated system assurance. **Where the national risk and threat profile requires, Member States can also implement a PWS that provides an integrated platform, which delivers both CB and LBSMS generated alerts**.

5.5 User organisations need to ensure that the PWS integrates with both their Control Rooms and the broader public information technologies. For example, through an Application Programming Interface (API), as done in Canada, it is possible for the PWS to update a public webpage, social media channel(s), radio and TV stations, etc., automatically with both the geographic warning area and message content[10].

5.6 A pivotal critical success factor is effective **community education**. This needs to be inclusive of all ages, from children to senior citizens. Warnings are only effective if authorities have explained their use **in advance**, so the community **understands** the significance of receiving an alert and the importance of **acting on the advice given**.

6. Lessons from other countries

6.1 Public Expectations

Experience from Australia shows the power of a national PWS in an emergency. In December 2014, the author conducted a post-implementation evaluation with Ipsos Australia. The survey canvassed views from communities and the emergency services to produce "The National Review of Emergency Alert". Its findings include:

- **A telephone alert is the preferred method by which the community wants to be alerted to an emergency.**
- **It is the official warning most likely to motivate households to evacuate or take other positive action required by the emergency services.**
- **48% of people surveyed said that an official telephone alert is their main trigger for action above all other public warning capabilities.**
- **80% of people who have received a telephone alert now expect to receive one for any future event.**
- **For those who rely on a single source for information in an emergency, 32% depend on their telephone for a warning, and**
- **82% of people surveyed stated that their "safety beats privacy" when it comes to telephone alerts.**

6.2 Social Media

6.2.1 This first case study illustrates why, in terms of compliance with Article 110 EECC, authorities cannot rely on social media. This is due to its current unacceptably high levels of discrimination against the vast majority of the population. Nevertheless, the principles of when and how the police, for example, use social media in an emergency is readily transferrable to using CB and/or LBSMS.

[9] COMAH: COntrol of Major Accident Hazards (Regulations 2015) – UK health and safety legislation.
[10] This is the approach taken by Canada with its National Alert Aggregation and Dissemination System.

Case Study 1: Social Media - London UK

Data	Population	% included	% excluded
UK Population	66.75 million		
Number of UK Twitter Users	17.1 million	26.6%	74.4%
London Population	8.78 million		
Number of @metpoliceuk Twitter followers in London	1.2 million	13%	87%
Number of @metpoliceuk Twitter followers in the UK	1.2 million	1.8%	98.2%
Number of international visitors to London annually	19 million		
Number of international visitors following @metpoliceuk	Unknown	?	?

6.3 Smartphone Applications

Both France and Australia have introduced Smartphone Applications (apps) in an attempt to warn and inform communities about emergencies on a local, regional and national scale. Whilst these provide a number of useful features that can be personalised, registrations remain a low percentage of the population. For example:

- **France** "SAIP": approximately 500,000 out of a national population of 67 million.
- **Australia** "VicEmergency": approximately 800,000 out of a state population of 6.3 million and a national population of 24.6 million.

Hence, apps will not comply with the requirements of Article 110 EECC.

6.4 Public Inclusivity/Access, Reach and Reliability

6.4.1 Article 110 EECC mandates that the PWS must be accessible to and reach the people affected within the warning area via their mobile phone. Public expectations are very likely to be that, when launched, from day one, the system will be non-discriminatory, accessible to and, every time, reach everyone with any type of mobile phone registering on any network within the affected area. **Thus, reaching everyone, everywhere, every time is the overarching critical design factor**.

6.4.2 It is worthy of note that Canada, USA and New Zealand have each rolled out a national PWS knowing from the outset that the chosen design (using CB) discriminates against people who, unwittingly, use an incompatible device. Hence, their types of PWS would not be fully compliant yet with Article 110(1) EECC.

6.4.3 The next case study is from the May 2018 nationwide tests of Canada's "Alert Ready" PWS. This was designed to be accessible to and reach only people with 4G mobile phones that are compatible with CB within a 4G coverage area. Thus, it excludes everyone without a compatible device and/or outside 4G coverage. Authorities[11] estimate that the test excluded over 70% of mobile phone users. Market analysts[12] assess that it may take between 5 and 10 years for the majority of Canada's population to upgrade to a CB compatible 4G device. **This creates significant legal liability issues for governments when they know from day one that the PWS will**

[11] Estimated by the Canadian Radio-Television Commission (CRTC).
[12] As stated by the system supplier, Pelmorex.

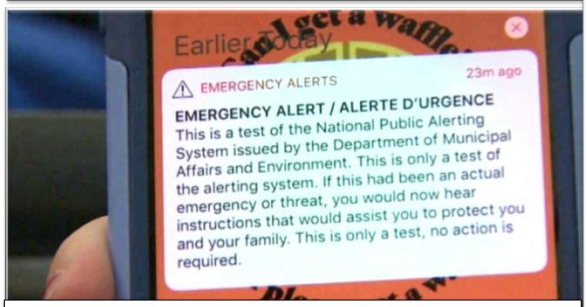
exclude a significant percentage of the population; particularly when it is the only viable means of alerting them.

Case Study 2: May 2018 - Canada

First Nationwide Test of the PWS

Glitches reported as emergency alert testing resumes across Canada

The same problems that affected Ontario on Monday are being seen across the country as tests continue



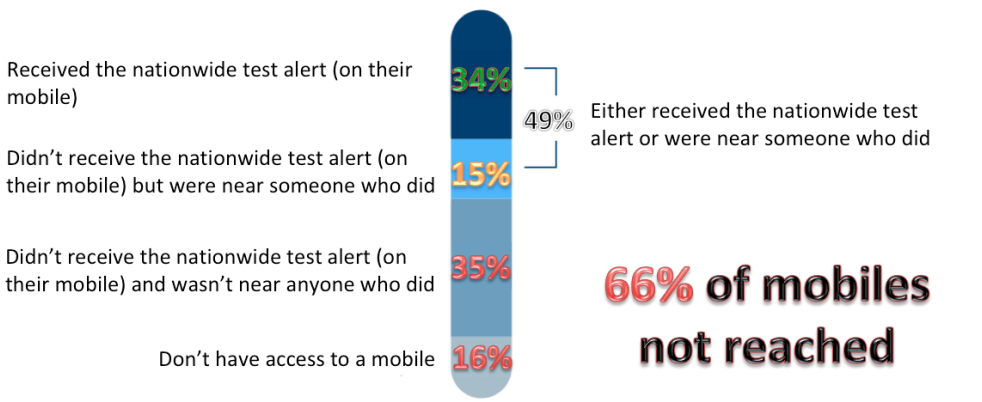
Broadcast received only on 4G compatible smartphones within 4G coverage. Other mobiles and those outside 4G coverage did not.

6.4.4 In the third case study, from New Zealand, authorities estimated that due to similar compatibility issues, their "Emergency Mobile Alert" PWS (that uses CB) reached only 34% of mobile phone users plus an additional 15% of the population (to whom the former passed on the alert).

Case Study 3: 26 November 2017 - New Zealand

First Nationwide Test of the PWS

One in three New Zealanders received the nationwide test alert Civil Defence sent from the Emergency Mobile Alert system on Sunday 26 November, and a further 15% were near someone who received the alert (but did not get it themselves).



6.5 Automated Near Real-Time System Assurance

6.5.1 Where the national risk and threat assessment includes large-scale disasters with a short time to impact and a degree of imprecision as to the area it will affect, such as,

- **Tsunami** (Chile),
- **Severe weather events** (USA and Canada);
- **Rocket attack** (Israel), or
- **Earthquake** (Japan and New Zealand),

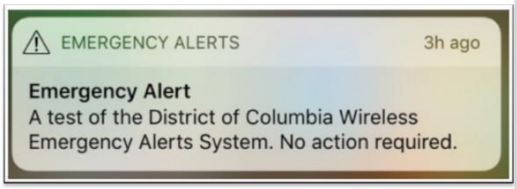
authorities in these countries have chosen CB. This is because it has a more rapid alerting capability than LBSMS for large-scale warnings, when "best endeavours" to warn at least some of the population (with a compatible mobile) to then alert others (who may not) is more important than the broader benefits and features of LBSMS.

6.5.2 In this next case study, from the first test of the "Wireless Emergency Alert" (WEA) PWS (CB) in Washington, authorities there (as well as Canada and New Zealand) rely on the public completing post-event questionnaires to assess PWS performance.

Case Study 4: 5 April 2018 - Washington DC, USA

First Citywide Test of the PWS

In first test of D.C. area emergency alert system, some phones beeped and buzzed. Others stayed silent.



"It was not immediately clear how successful the exercise was…Now we need people to take our survey and answer some questions."
Office of Emergency Management

6.5.3 EU Member States will need to establish whether their authorities have a requirement for automated, near real-time system assurance for more localised, day-to-day emergencies. In these instances, authorities may want to know immediately how many people/mobile phones are within the area affected, and whether the system delivered the warning message to them successfully. Only LBSMS can provide this.

6.6 Granularity of the Warning Area

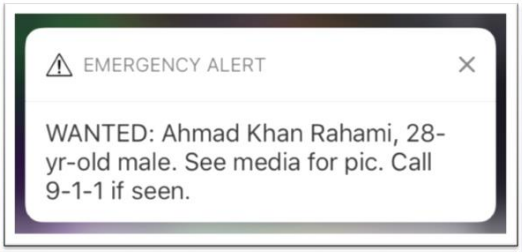
6.6.1 Limiting the alert area only to those people immediately affected and/or at risk is a critical requirement in a range of operational scenarios. This would include a marauding terrorist attack, active shooter, gas leak, and a building evacuation. In these instances, and subject to the local network configuration, police will want to restrict the warning dissemination to a narrowly defined geographical area, potentially, down to a single building or block of streets.

6.6.2 This fifth case study was the first time authorities in New York City, USA, used the WEA PWS to alert citizens to a terrorist fugitive. They had intended the warning to go only to people in the suburb of Chelsea. Instead, the CB platform disseminated the message to every compatible mobile across the whole of Manhattan. In addition, as the commentary reflects, they failed to structure the message content in accordance

with the international standards set by the "Common Alerting Protocol (CAP)[13]". This is designed to enable the public to know which authority sent the message; understand the threat; how it affects them; the area at risk, and the action to take.

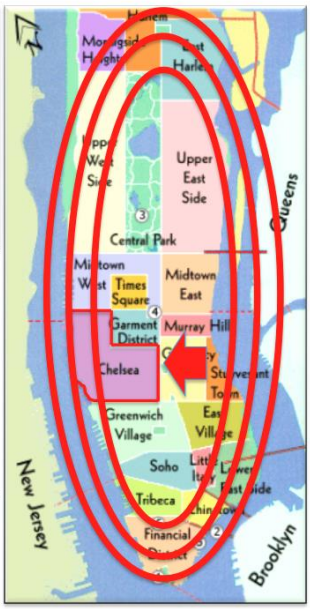
Case Study 5: 19 September 2016 - New York City

First Use of WEAS in USA to Locate a Fugitive



That's it. No links, no pictures, no further context—no one to call except 911. I got the alert while feeding my toddler breakfast, and in my pre-coffee haze, I glanced at my phone and mistook it for an Amber Alert. Elsewhere in the city, subway cars full of people must have looked up from their phones and regarded one another warily. Might one of their fellow passengers be Ahmad Khan Rahami? Young men with brown skin might well have wondered: Might one of my fellow passengers *mistake* me for Ahmad Khan Rahami? William Oremus

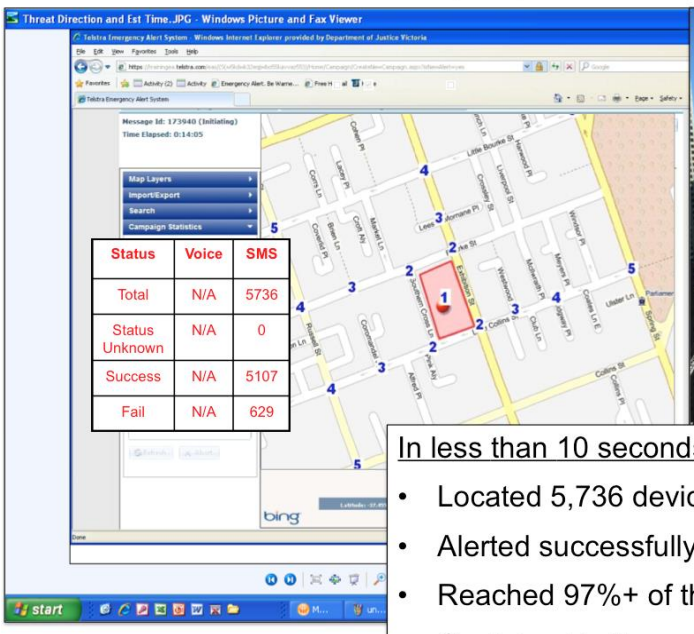
Broadcast only to compatible smartphones across the whole city rather than just to those within the warning area.

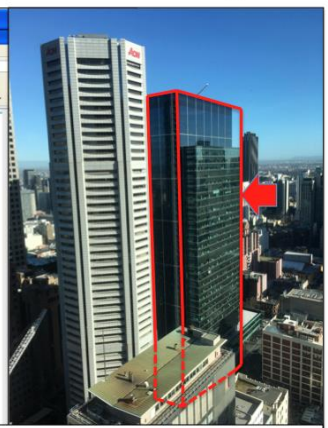


6.6.3 By contrast, in the final case study, authorities in Victoria, Australia, utilised the "Emergency Alert" (LBSMS) PWS for an evacuation exercise to alert only the people in a 37-storey office block, the Department of Justice Building, in Melbourne.

Case Study 6: 14 December 2012 - Melbourne

Evacuation Exercise – 37-storey Department of Justice building





In less than 10 seconds:

- Located 5,736 devices
- Alerted successfully 5,107 mobiles
- Reached 97%+ of the people
- Contained to the warning area.

[13] http://www.wmo.int/pages/prog/amp/pwsp/CommonAlertProtocal_en.html

The system located all 5,736 devices registered on the three networks inside that building. The total included 629 non-mobile telephone handsets, such as tablets. The alert successfully reached all 5,107 mobile phones and, thereby, more than 97% of the people within the building. Mobile phones outside the warning area did not receive the alert. CB has not been tested successfully to deliver the same capability.

6.6.4 To achieve this level of granularity is entirely dependent on the configuration of the local network in a metropolitan environment. It may not be possible to replicate the Australian example at every location and certainly not in rural areas. Thus, the warning area may need to be expanded to be sure of reaching everyone within the actual area affected.

6.6.5 Like Belgium, with the early successes of its "BE-Alert" PWS, both Iceland and Australia chose LBSMS as an expandable and future-proof technology. It is compatible with every mobile manufactured worldwide and, thus, fully inclusive on the 2G (now switched off in Australia), 3G, 4G and the future 5G networks. The system incorporates automated performance assurance. This enables the operator to view on-screen in near real-time only the **aggregated and anonymised totals** for:

- The number of mobiles/devices registered simultaneously within coverage on every network for the geographically defined warning area, and
- The numbers of mobiles that then received the alert successfully or not.

The operator is not able to view the individual mobile phone numbers.

7. Access to Personal Communications Data

7.1 The question of whether authorities require access to personal communications data for the purposes of public alerting will be one of the most significant political and operational matters for EU Member States to consider. It will determine the choice of PWS technology and, thus, extent of the capability, functionality and public safety features available.

7.2 Authorities must weigh up the long-term benefits and disbenefits to public safety, national security and disaster management of whether or not to allow automated access to the data in an emergency. In the interests of saving life, one approach is to have simplified but clearly prescriptive legislative controls on when and how to access the data solely for the purposes of public alerting (that are different to investigations).

7.3 CB does not require access to data, as it is just a broadcast on the signalling channel. LBSMS does require access to locate all mobiles in the affected area, alert them and confirm delivery of the SMS warning. The types of data the LBSMS PWS can utilise for public safety include:

1. **Cell ID** for the cellsite/sub-cell on which the mobile last registered[14]
2. **Latitude and longitude** of the device from the network when it last registered
3. **GPS position** from the smartphone when it last registered
4. **MSISDN** (phone number)
5. **IMSI** (SIM card number)
6. **IMEI** (equipment identifier), and
7. **SMS delivery receipt** and/or failure.

7.4 1, 2 and 3 are critical to identifying when a mobile telephone is/was within coverage of the defined warning area.

[14] This is the "Last Known Location (LKL)" and is based on the most recent transaction between the device and the network. When the mobile is left switched on and there is no activity; e.g. while the user is asleep, the device updates the Mobile Network Operator with its LKL automatically every 60 minutes. By comparison, Cell Broadcast disseminates the alert to every compatible device currently registered at that time on the relevant cell sites giving coverage into/within the warning area.

7.5 4, 5, 6 and 7 are vital to the successful performance monitoring and assurance of the PWS automatically and in near real-time. In addition, the IMSI can identify the user's country of origin (for the warning content language). The IMEI enables the PWS to filter out all non-mobile telephone devices. The MSISDN enables the emergency services to utilise other critical features, without which the benefits of an all hazards, all agencies capability will be diminished significantly.

7.6 There are a number of modalities for he PWS to access personal communications data. These include (but not limited to) all data remaining within each Mobile Network Operator's systems. The PWS operator can view on screen only a set of anonymised aggregated totals (as explained in 6.6.5). The latter can overcome public concerns about data privacy, albeit the Australian experience shows that 82% of the population put personal safety above privacy (see 6.1).

8. Operational Context and Value

8.1 The principal value of the PWS is its capability to help the emergency services save life and protect livelihoods. No greater value can be placed on such a system. In Australia, since the introduction of the "Emergency Alert Location Based Solution" (LBSMS) in 2012, no more lives have been lost due to an inability to warn. Early warnings also add value by helping people reduce, if not, prevent avoidable losses, thereby minimising the costs of personal injuries and subsequent insurance claims, as well as aiding business resilience and continuity. Thus, in determining the cost of implementing the PWS, authorities need to assess that figure along with the value-adds from its benefits to community safety, and balance them against the cost and public liability of delivering a sub-optimal capability, or doing nothing.

8.2 Countries with a PWS deployed already have integrated the capability into their Control Rooms. This ensures that alerting the community is integral to the early response to an emergency. As discussed previously, the PWS provides a fast, safe and highly efficient means of remote "door-knocking". On 14 June 2017, such a system would have had significant benefits to assist the London Fire Brigade within seconds to reach and alert people automatically on all 24 floors of Grenfell Tower of the decision to evacuate.

8.3 On 5 July 2018, Lord Toby Harris of Haringey addressed the (UK) House of Lords on the subject of public alerting and made the following observation,

"Two weeks ago, Michael Dowden, the London Fire Brigade watch manager for North Kensington gave evidence to the Grenfell Tower inquiry and said:

"For me … to facilitate and change a stay-put policy to a full evacuation was impossible. I didn't have the resource at that time. We're looking at 20 floors above the fire … I just don't know how that could have been done with the resources we had in attendance at that moment in time".

Tragically, the technology to deliver that message to those waiting in their flats exists and, had it been adopted in this country, could have been used on that terrible night."

72 people died in the Grenfell Tower fire.

8.4 Whilst the system cannot yet be floor-specific, the message content can include advice on the action, timing and route for people on each floor.

8.5 In December 2014, the police in Perth, Western Australia, used "Emergency Alert" to ask the public for help to search for a 3-year-old boy who had gone missing in a local park. In response, 500 volunteers arrived at the police station. The boy was located within 25 minutes, thus minimising distress to the family.

9. Conclusions

9.1 Whilst it is unlikely that there will be a one-size-fits-all approach that suits every EU Member State, there will be many synergies in terms of functional requirements, policy, legislation and operational procedures. These provide opportunities for close collaboration, as well as economies of scale, to help accelerate the design, development and implementation phases at a reduced cost to each State.

9.2 With regard to choosing the right technology, Member States must be cognisant that, whilst their sovereign borders are physical, national mobile phone networks can roam up to 35Kms into neighbouring territories. Similarly, with regard to Recital 260ab EECC, major emergencies and disasters can cross national borders. Hence, Member States need to choose a technology that is both accessible to and reaches equally both their citizens and international visitors via their choice of mobile device.

9.3 When reviewing the value of the investment in the PWS, it is worth considering Australia's experience. The national system cost in the region of €67 million[15]. The cost to one state in loss of life and consequent legal action for a perceived "failure to warn" was significantly greater, €133 million ($150M AUD) out of a total €600 million ($794M AUD) settlement against both the power utility companies and the state government. "Emergency Alert" is a lasting legacy to the memory of the 173 lives lost on "Black Saturday" (7 February 2009) that triggered its introduction.

9.4 To generate the greatest return on investment, EU Member States need to consider the value of creating one community safety ecosystem that provides a common platform, built on an enterprise architecture for public safety, disaster management and national security. The objective is to maximise the availability of relevant data for multiple purposes as an all hazards, all agencies capability.

9.5 The project to design each EU Member State's PWS platform needs to follow the sequential discipline of,

1. **People**: what we need to achieve - to determine the community safety outcomes and expectations from the system to identify its functional and operational requirements for all its user authorities.
2. **Process**: when and how we will use the system - to establish the standard operating procedures, policies and legal frameworks from which to train personnel in the relevant user authorities, and educate the community, and
3. **Technology**: to evaluate available technologies against the People and Process elements - to determine which best meets **all** the essential requirements.

9.6 Future PSCE workshops to support implementation of Article 110 EECC will look at the potential for collaboration on a range of common work-streams to develop:

- Integration with existing Control Room processes and systems
- Community education, awareness, marketing and communication
- Operational readiness
- Accessing personal data and enabling legislation
- Cross-border interoperability and standards.

[15] Much of the cost to Australia was due to pioneering the research and development. Today, the equivalent WEAS can be delivered as a sustainable, less expensive off-the-shelf managed service.

9.7 In those countries that have implemented the capability already, their PWS is a proven life-saver. The experiences and advice offered in this White Paper will assist every EU Member State to advance the development of its project, from design through to delivery within the 42-month deadline set by Article 110 EECC. The objective is to get it right first time and, thus, provide lasting benefits to public safety and security from the outset.

About the Author

Michael Hallowes is the former **Emergency Services Commissioner** for the state of Victoria, and **National Director of Australia's "Emergency Alert Program"** (2011 to 2015). He oversaw design to delivery of the national LBSMS PWS, known as the "Emergency Alert Location Based Solution", which is fully compliant with Article 110 EECC.

He is now the Managing Director of ***Zefonar Advisory Limited***. This is a UK registered consultancy that brings together an international alliance of respected public alerting practitioners and operational transformation specialists to deliver unequalled solution design services for public alerting.

This paper is based on the author's extensive, hands-on experience from leading Australia's equivalent PWS project, and its post-implementation administration and evaluation.

Australia's equivalent PWS, "Emergency Alert Location Based Solution"

Since its introduction in 2012, emergency services across Australia have trusted the system:

- in more than **1,400 campaigns involving localised and large-scale events**,
- to send in excess of **14 million alerts successfully by SMS**.
- "Emergency Alert" has a proven reliability, with an overall average success rate per campaign of **reaching 97%**[16] **of mobile phones** on the 2G, 3G and 4G networks in the affected area.

The largest campaign involved the successful delivery of more than 800,000 alerts, the smallest, less than 500. Since implementation, there has been **no more loss of life** in Australia due to an inability of the emergency services to warn the people affected.

Today, a LBSMS PWS can deliver securely up to **10,000 alerts by SMS per second**[17]. There is no evidence of SMS alerts congesting the networks.

[16] The other 3% represents the early system design when it had no ability to filter out non-mobile telephone devices also registered and visible on the networks. Today, unlike Cell Broadcast, **LBSMS is accessible to and can reach 100% of all mobiles manufactured worldwide**. LBSMS platforms are also **5G-ready**.

[17] As proven on the STC network in Mecca, Saudi Arabia for crowd safety alerts during the 2018 Hajj. The average overall size for each campaign exceeded 1 million SMS without congesting the networks. Australia's LBSMS platform is calibrated to send up to 500 SMS per second. Given the average overall campaign size across all the states and territories is around 5,000 mobiles, Australia has chosen so far not to expand the capacity of the system and SMSCs, nor has it seen the operational need to add CB to the "Emergency Alert" platform. The latter includes a service address-based feature for mobiles and landlines, known as the Location Based Number Store, which was Phase 1 of the system design. Australia is now on Phase 4 in readiness for 5G.