**Timothy Compston** looks at how mass notification technologies are keeping people informed when the worst happens

# ON ALERT AND RE

When a terrorist attack strikes, or there is some sort of natural disaster, the ability to communicate in an effective and timely manner with those in harm's way is a critical consideration. As we have seen with events in Paris, Brussels and more recently in Nice and New York/New Jersey, situations can develop extremely quickly and, in some cases, impact more than one location simultaneously, adding to the fear and confusion on the ground. In addition to the authorities employing social and more traditional media to reach the public and other stakeholders with their messages, we are witnessing a new generation of specialised solutions coming to the fore that are designed to deliver targeted, geo-specific information in a joined-up way.

One approach that has certainly gained more traction over recent years, with mixed results, is specific smartphone applications or apps. In the lead-up to the Euro 2016 tournament in France, for example, a major concern was how to communicate safety and security messages should a terrorist-type situation develop. The solution in question was a free emergency app known as SAIP – which some dubbed 'the terror app' – whose origins can be traced to the Paris attacks last year.

A major test for SAIP came not at Euro 2016 itself but soon after when, on Bastille Day, a truck was driven into crowds in Nice killing over 80 people and injuring hundreds more. Unfortunately, according to media reports at the time, the app – which was designed to flash an 'instant' warning on a user's mobile phone screen if an attack was close to their location – failed at the first hurdle. In fact the initial notification was only issued at 1.34 am, more than three hours after the attack had actually started. In a follow-up story, shedding more light on what transpired, *Les Echos* newspaper said that a message prepared by the local prefecture was actually ready at around 11.15 pm but, worryingly, a technical glitch prevented the app sending out the warning.

Speaking to Imad Mouline, cto at Everbridge – the enterprise software company that creates applications to automate the delivery of critical information – for his thoughts on the failure in Nice, he believes that it serves to reinforce the case for the implementation of multiple communication routes: "Many things have evolved, but one thing that hasn't is that communications are likely to break down at some point. There probably has not been a major event or an incident where there hasn't been some level of communication breakdown". The problem, says Mouline, is that it simply is not possible to anticipate where a communication issue will fall ahead of time: "During Hurricane Sandy, some parts on New Jersey lost cell towers so mobile phones were inoperable and in other parts of New York, for example, landline calls couldn't get through because central offices were

overwhelmed. Post Paris, the French Government commissioned a nationwide application for smartphones so people could receive push notifications. When they activated it [the app] after Nice that was a pretty big failure. Alerts were delayed across the board – by hours – which for an event taking a few minutes to come to a conclusion becomes an issue".

Given the reality that no communication path is 100 percent reliable – 100 percent of the time – Mouline reiterates the view that the only way to increase the chances of reaching out to people, and hearing back from them, is to adopt a multi-modal approach: "It is

# EADY FOR ACTION

about having as many ways of communicating with people as possible because you don't know what is going to work and what is not going to work".

Talking to Darren Chalmers-Stevens the director for EMEA at Critical Arc – which develops distributed command and control solutions for large-scale sites like University campuses – about how things have changed on the mass notification front, he agrees with the point about the advisability of no longer being reliant simply on one single communication mode: "At the top level, the first thing has to be multi-layered communications, so hitting someone with at least two or three forms of communication". For Chalmers-Stevens, this communication can be via SMS, email and, importantly, push notification, which he points out is free and secure.

Chalmers-Stevens adds that the ability to link into social media is also beneficial here: "Having an API [Application Programming Interface] available so you can tie in to an organisation's social media platforms allows you to get the message out in multiple forms of communication". Alongside this, he points to desirability of SIP – phone system – integration: "In essence you can broadcast messages both in traditional terms, but leverage the entire phone system internally to send a broadcast message over an IP phone".

Chalmers-Stevens admits that there is never going to be the complete uptake of a message by everyone, but that by taking what he refers to as a 'funnel' approach, hopefully the majority can be reached: "If you get into a scenario where you have a room [in a university] at least a percentage of that room is capable of receiving that message and they can then act in this social environment to share that information with their colleagues".

Looking back at the issues that traditional systems typically threw up for users, and which the latest mass notification solutions have sought to overcome, Chalmers-Stevens says that it has been good to move away from an over reliance on SMS: "Using SMS is obviously costly, so universities [for example] were having to make a judgement call, do I want to send a message to 10,000 students? That [sending an SMS] is going to be a fair cost and people sometimes were assessing cost versus risk and that was a terrible predicament for them to be put into".

Another concern that Chalmers-Stevens is keen to bring to the table relates to the fact that some public sector concerns had and still have quite a rigid approvals process for communications: "This means that certain individuals have to be engaged and sign off on something being sent to more than a small group of users. That, unbelievably, can sometimes delay sending out broadcast messages to tens of thousands of users by hours, when they are trying to chase down individuals that can make the decision to send things out on the fly".

Alongside this, Chalmers-Stevens says that another problematic issue is the fact that many older systems are just standalone: "There is not any tie-in to operational data and where assets – like first aiders – actually are. In essence you are then broadcasting messages out to everyone and that has two consequences, one is that it draws people to a situation that they don't necessarily need to be involved in and it adds additional pressure to the security team". To illustrate his point, Chalmers-Stevens cites the example of the coffee shop attack in Sydney, Australia, back in 2014: "People got notified of the scenario in terms of the traditional media outlets

# ON ALERT AND READY FOR ACTION

and started going to the location and streaming onto Facebook, which was horrendous for those seeking to manage the situation. If you are trying to control things and have the best outcomes, you don't give publicity to potential terrorist attackers".

So how can some of the issues Chalmers-Stevens has raised be addressed? In addition to the multi-layered communications touched on earlier, he says that it is important to look at targeted messages: "This is about creating groups within the system. So it could be buildings, faculties, departments or business groups like gold, silver, and bronze command structures".

Moving to a unified platform rather than standalone can also pay dividends says Chalmers-Stevens: "You are trying to make it as easy as possible. If you look at a traditional SMS platform or even up-to-date 'mass coms' systems, they are standalone systems with no incentive for the user to download or actually maintain them. We all know that we are pressured for space on our smartphones in terms of data storage, so an app is liable to be culled if it is just one service". Chalmers-Stevens reckons that the addition of functionalities like a panic button, a first aid request option and even a 'transport tracker' has certainly helped take up among students in the university arena where Critical Arc and its SafeZone solution has the biggest footprint.

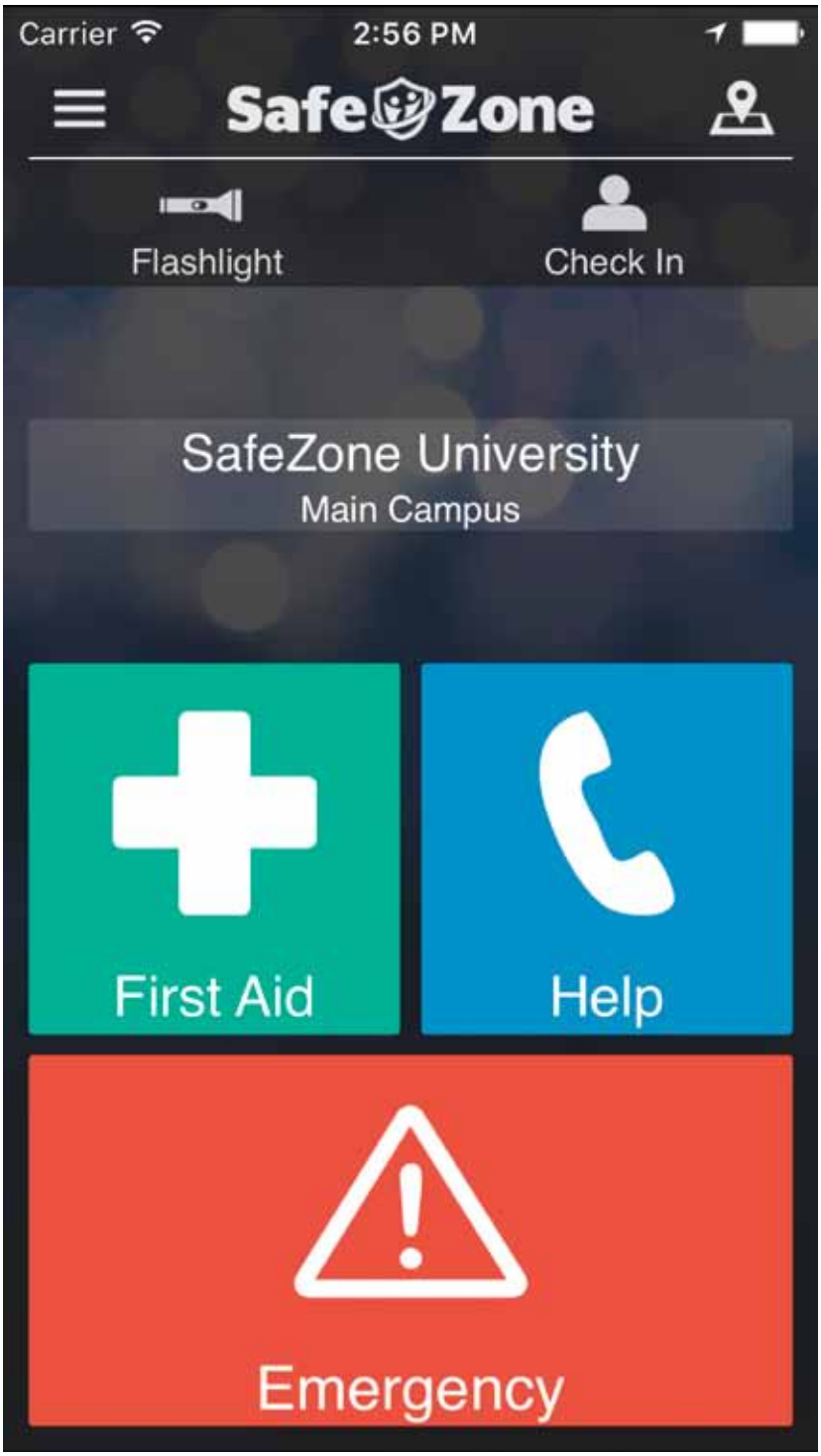
Turning once again to the thoughts of Imad Mouline – cto at Everbridge – he believes that as well as sending information out, on the other side of the coin, it is vital for those in charge when a dangerous situation strikes a city, for instance, to be in a good position to appreciate what is coming in too: "In the assessment stage there is information coming back or being offered up from the frontlines, the residents the employees of offices telling you what is going on, whether you solicited the information or because they are the first ones to see it. You have to create a framework that allows them to provide that information and to have that information automatically, if at all possible, categorised and analysed so as not to overwhelm the authorities".

Rewinding to recent events in New York/New Jersey – which saw a pressure cooker filled with shrapnel explode, and the eventual arrest of Ahmad Khan Rahami – Nick Hawkins, managing director EMEA at Everbridge, confirms that public safety officials in Linden, New Jersey, were able to take advantage of Everbridge's Nixle notification system to deliver an alert to community members that offered quick, detailed, information about the suspect's appearance, and his role in the bombing. This led to Ahmad Khan Rahami's discovery and arrest in Linden less than two hours after the initial alert. With Everbridge Nixle in place, residents have the ability to anonymously share critical information with agencies via text or online submissions and agencies can automatically post alerts to multiple social media channels, saving valuable time and resources while expanding resident reach.

Nick Hawkins, goes on to say that, in his experience, the US market is still more open to this type of communication compared to here in the UK: "The acceptance that you will be communicated with around an incident such as this [New Jersey] seems to be part of everyday life. We also saw this with the Boston bombing in 2013 where we [Everbridge] provided a similar technology to organisations and government institutions to communicate with people along the lines of 'don't come into the city' or go to a place of safety".

In the end, when it comes to communicating and receiving information about fast moving incidents, like terrorism, authorities or site owners need to ensure that they have redundancy built-in to their communication channels and, crucially, that any tailored messages are targeted at the right people and places.

***CriticalArc's SafeZone app is used in universities for contacting large numbers of people en masse***




©CriticalArc

**Timothy Compston** is a journalist and security professional that specialises in security issues. He studied International Relations and Strategic Studies at Lancaster University, is PR director at Compston PR and a previous chairman of both the National Committee and CCTV PR Committee of the British Security Industry Association.