Enhancing the efficiency of alerting systems through personalized, culturally sensitive multi-channel communication

Project No. 261699

Deliverable D7.3

"Discussion of privacy issues with end-users"

Contributing Partner(s):

Nederlands Instituut Fysieke Veiligheid Nibra (NIFV)

Regione Sicilia, Civil Protection (SIC)

Introduction

The concept of the Opti-Alert project, a personalized, socio-culturally sensitive alerting strategy and tool, automatically entails data protection and privacy issues. In D7.1 the legal framework (both on the European and national level) with regard to these issues of the Opti-Alert project has been reviewed. In D7.2 the privacy aspects of the data previously (WP2) identified as relevant for the Opti-Alert system have been assessed; criteria were, including sensitivity (according to EU directives) and influence on potential identification of an individual. In the present report the results of discussions of these privacy aspects with potential end users of the Opti-Alert system are presented.

For this deliverable end-users like (operational) crisis communication officers and crisis managers have been interviewed in Italy and the Netherlands. There are many similarities between these two countries.

Perception

End users acknowledge potential privacy issues in crisis communication. At the same time they indicate that these issues don't have the highest priority during a crisis. "Necessity knows no law" is the motto. Sometimes there is a balance of interests between fast acting and adequately informing the public on the one hand and a careful consideration of privacy interests on the other hand. Ultimately it is the "supreme commander" of the crisis management (usually the mayor) who will decide whether privacy or fast acting prevails. In practice, according to literature and the end users interviewed, this dilemma has never led to problems.

Kinds of privacy issues

For the purpose of crisis management situations, public authorities can decide to communicate to the public for several reasons: not only, for example, to provide the people with information or to warn people, but also to obtain assistance from people.

There can be privacy issues in crisis communication in two ways:

1. information about people is communicated (e.g. names of victims)
2. databases with personal details are used:
    a. existing databases designed for other purposes
    b. existing databases especially designed for use in crisis management

Ad 1. Regarding the first point, general policy is to show restraint in publishing information about people. In principle, names of individuals will never be communicated in the media, unless the identity of these people is beyond dispute. Communication of false information must be prevented at all cost.

This policy cannot always be maintained, because sometimes information about victims is communicated 'informally' via social media. In such a case a more flexible approach in the 'official' communication is chosen. This was, for example, the case with communication about the Dutch victims of the aircraft crash in Tripoli (2010).

Ad 2a. On the second point: when a message needs to be directed to a specific audience (such as people of a certain ethnicity, or elderly, young or disabled people), the obvious information about these individuals (such as name, phone number, address) can be found by consulting the available databases. Thus, a message can be very specifically addressed.

In the Netherlands and Italy some databases containing a lot of information potentially useful for this purpose are available. In the Netherlands for example you have the 'Gemeentelijke Basisadministratie' (GBA: Municipal Registration) and the 'Basisregistratie Adressen en Gebouwen' (BAG: Registration Addresses and Buildings) which contains information about (the use of) specific buildings. The information available in the various databases could be made even more useful by combining the databases.

In times of crisis such information can be used to address alerting messages to specific individuals or groups of people, for example inhabitants of a retirement home or children attending a specific school. Although one has to face some privacy issues (as indicated in D7.1 and D7.2), it is possible to use those databases for crisis communication. In practice, this is never the approach of choice in Italy, nor in the Netherlands. Instead, alerting messages are communicated widely (by a multi channel approach). Thus, privacy issues are avoided. This approach will lead to many more people (than just the target group) receiving the message, however this is not considered as a problem. When an incident occurs in a certain part of a city, the government can quite easily see whether that neighbourhood has certain sociological and cultural characteristics. In the Netherlands, this information is freely available via the Internet (www.cbsinuwbuurt.nl). Based on this information, the communication can be tuned to the community in that neighborhood (for example, reports in Turkish or Arabic). However, the communication will not be specifically addressed to (a group of) individuals.

Moreover, experts expect that the method of crisis management will increasingly change. The government will increasingly less determine who should get what information, instead they will more and more assume a supportive role in crisis communications. Citizens will increasingly search for information and will decide themselves which information is relevant to them and which is not. Social media will help to accelerate this process.

At the same time, Opti-Alert Work Package 2 (D2.5) shows that many people (still) rely on 'traditional' communication and media in times of crisis and don't expect to use social media or even the Internet in times of crisis. Governmental organizations will have to put more effort in the communication to and alerting of those people. In that case it might be helpful to know something about these individuals. Thus, in contrast to the approach of choice described above, it is possible that communication experts will decide to send different messages to different socio-cultural groups, using freely accessible databases originally designed for other purposes, such as the Dutch GBA and BAG.

Ad 2b. A final privacy issue concerns collecting data about and/or from people specifically for crisis communication. By obtaining information about people and/or having people give information about themselves in advance, communication during crises can be highly targeted. The Netherlands have warning systems for assistance from citizens in the detection of missing children ('Amber Alert') and detection of criminal offenses ('Burgernet'). For participation in

these systems citizens volunteer. They will receive a message on their mobile phone when a child is missing (Amber Alert) or when the police in the region where they live invokes the help of citizens in the detection of an offense (Burgernet). For Amber Alert, no personal data of the participants are registered. For Burgernet details of participants are registered, such as name, date of birth and residential address. These data are registered according to the standard privacy laws and regulations.