Project acronym:	COSMIC
Project title:	The COntribution of Social Media In Crisis management
Grant number:	312737
Programme:	Seventh Framework Programme – Security Research
Objective:	SEC-2012.6.1-3
Contract type:	Coordination and support action
Start date of project:	01 April 2013
Duration:	24 months
Website:	www.cosmic-project.eu

Deliverable D3.21

Political, social and industrial opportunities arising from the use of emerging technologies

Author(s):	Ioannis Kotsiopoulos & Angelos Yannopoulos (ED); Hayley Watson, Rachel Finn & Kush Wadhwa (TRI); Alex Papadimitriou (HRT)
Dissemination level:	Public
Deliverable type:	Final
Version:	1
Submission date:	Due 31st October 2013

Table of Contents

Change Records

Issue	Date	Description	Author (Company)
0.1	29/10/2013	Draft received from internal review	Alex Papadimitriou (HRT)
0.2	31/10/2013	Final version submitted	Ioannis Kotsiopoulos (ED)

EXECUTIVE SUMMARY

The present document is the first version of the deliverable "Report on the political, social and industrial opportunities arising from the use of emerging technologies" (D3.21) of the COSMIC Support Action. The purpose is to look into the political, social and industrial implications of the use of emerging technologies in crisis situations, in relation to existing policies and standards for the development and use of such technologies, as well as to highlight the opportunities which may arise for industrial stakeholders and the general public. We also address the inherent challenges and limitations posed by privacy and security issues, in the context of mass utilisation of emerging technologies and information gathering/sharing.

On the policy front, we present applicable measures and current EU legislation such as the Directive on data protection and the "Telecommunications Package". Proposed reforms in existing legislation in areas such as data protection and the role of the Universal Provider in telecommunication services are presented from the point of view of their effects on crisis-laden social networks services. In a similar fashion, we examine EU policy directions on emerging issues such as the openness of the Internet and the freedom of citizens to access and run applications and content.

With regard to standardisation we identify challenges such as the underlying telecommunications technologies, the presentation layer of social media, the data involved and the means of interacting with social media services. For the latter, we draw attention to the complex interplay between market leaders and their competitors and correspondingly between proprietary and open standards.

Moving on to the subject of privacy and security, we identify and discuss the various privacy-related issues for stakeholders to consider, including transparency, legitimate purpose, data protection, anonymity and the impact of data collection on surveillance. In addition, we consider the various challenges surrounding the protection of information as well as the potential impact of the use of new media technologies on citizens' safety. Our findings point to the need for added measures by organisations (and possibly members of the public) with the aim to protect those with whom they are interacting.

This analysis will be further developed within the COSMIC project as part of our on-going work into the various social opportunities and challenges regarding the use of new media applications in crisis management. Additional aspects that will be investigated in the final deliverable (D3.22) will include counter-surveillance (especially against misuse of power by security officials during political crises), lateral surveillance for emergency response, and utilisation of social media for mobilisation and organisation of social activists.

1 INTRODUCTION

Understanding the contribution of social media and other (relevant) new media applications in crisis management requires an examination of the political, social and industrial considerations of existing and emerging technologies, including social networking sites such as Facebook and Twitter for crisis management. By doing so, partners will explore political, social and industrial opportunities and challenges concerning the use of existing and emerging new media applications in crisis management activities. The findings of this work will go some way to informing our recommendations and guidelines in workpackage 6.

The present deliverable, a preliminary report, D3.21 "Report on the political, social and industrial opportunities from the use of emerging technologies" contains four chapters. In addition to the introduction, chapter 2, explores existing policies, standards and opportunities relating to the use of emerging technologies in crisis situations. Partners will focus their efforts on identifying existing policies and standards for the development and use of social media oriented technologies as well as on examining any opportunities that may arise for industrial stakeholders and the public. Specifically, partners will explore legislation around data protection, telecommunications and other (relevant) upcoming EU developments such as updates of existing Directives and policy directions contained in the Digital Agenda.

Chapter 3 of this report will examine the challenges associated with privacy and security when utilising new media applications, particularly social media, as part of crisis management activities. Such challenges include: awareness of and appropriate consideration of EU policies on privacy and data protection, the need for transparency in operations, data protection considerations, the ability to maintain the anonymity of individuals during the sharing of data and the secondary use of data. The chapters' preliminary investigation into security issues include: protection of information from loss or theft, reliability and accuracy of information and vigilante justice.

The report concludes in Chapter 4, where partners summarise the most important findings concerning the role of social media in crisis management, in areas such as applicable legislation in the EU, policy directions, the standards landscape and the privacy and security related challenges arising.

This deliverable is an on-going piece of work and will be completed in July 2014 via Deliverable 3.22 "Final report on the political, social and industrial opportunities from the use of emerging technologies".

2 EXISTING POLICIES, STANDARDS AND OPPORTUNITIES

The chapter will examine the political, social and industrial implications of the use of emerging technologies for crisis situations. At this first stage, partners will focus on the identification of existing policies and standards for the development and use of such technologies as well as the opportunities which may arise for policy makers, industrial stakeholders and the general public. The first part of this chapter provides an overview of policies which at European level affect social media, followed by a discussion on the role of standardisation and its use in relevant emerging technologies.

2.1 POLICIES AT EUROPEAN LEVEL

We examine the policy framework at the European level with regards to issues akin to social media, such as the protection of personal data, the provision of bandwidth for the operation of social media sites, Internet openness and neutrality, and interoperability.

2.1.1 Personal data

Although the privacy of citizens must be respected and protected by law, this must not become a hindrance to the free movement of voluntarily supplied personal data, which is an essential element of social networks.

As presented in the Europa website[1], Directive 95/46/EC[2] is the reference text, at European level, on the protection of personal data. The Directive comprises of a regulatory framework to balance the protection of privacy for individuals against free movement of personal data within the European Union (EU). The main features include strict limitations on the collection and use of personal data and the obligation of Member States to establish an overseeing body operating independently at the national level.

Although the Directive concerns data processed by automated and manual means, its application does not include activities not covered by the Community Law (such as public security, defence or state security) and the processing of data by individuals (called “natural persons” in the Directive) for purely personal or household activities.

The Directive outlines guidelines with respect to the processing of personal data by taking into account factors such as:

- the **quality** of the data, which must be accurate, up to date, lawfully and fairly processed and collected
- the **legitimacy** of the processing, and the consent of the data subject
- the exclusion of special **categories** of processing, such as information regarding racial or ethnic origin, political opinions, beliefs, medical data and others
- the **information** given to the data subject, such as for example the identity of the data processor, his purpose etc.
- the data subject's **right of access** to data kept relating to him/her
- **exemptions and restrictions**: on matters such as national security, defence, public security, prosecution of criminal offences and others

[1] http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm

[2] EUR-Lex, access to European Union law, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT

- the **right to object** to the processing of data
- the **confidentiality** and security of processing
- the **notification** of processing to a supervisory authority

The data protection Directive (including amending Acts such as Regulation (EC) No 1882/2003[3]) is currently undergoing an update process. As described in the dedicated Commission's mini-site[4], advances in the Internet and the way the personal data landscape has changed since the adoption of the Directive (1995), via technologies such as eCommerce, social networks, online games and cloud computing, have highlighted the need for strengthening protection of personal online data. Key changes proposed by the Commission are:

1. Guaranteeing easy access to one's own data and the freedom to transfer personal data from one service provider to another.
2. Establishing the **right to be forgotten** to help people better manage data protection risks online. When individuals no longer want their data to be processed and there are no legitimate grounds for retaining it, the data will be deleted.
3. Ensuring that whenever the consent of the individual is required for the processing of their personal data, it is always given explicitly
4. Ensuring a single set of rules applicable across the EU.
5. Clear rules on when EU law applies to data controllers outside the EU

The new proposals are currently under debate by the Council and the European Parliament. We draw attention to proposal two, due to its significance to social networks. As data exchanged via these networks grows larger and larger, so does information related to each member of such a network. Given that the most popular of these networks (such as Twitter, Facebook and others) have evolved into private companies, the amount of personal data held by them can be disproportionately large. The example of the Austrian student who requested the information held on him by Facebook, quoted in the Commission's factsheet[5], is illuminating: 1224 pages were sent to the requestor, much of which he himself had deleted. The "right to be forgotten" or the "right to oblivion", as it is also called, contained in Article 17 of the proposed legislation[6], serves this purpose. The Eurobarometer 359 findings (June 2011) quoted in the same factsheet show that only 26% of social network users and even fewer online shoppers (18%) feel in complete control of their data.

One should note that not every country or stakeholder concerned agrees with the proposed article 17. Among them is the UK, whose Ministry of Justice is of the opinion that the very phrase "right to be forgotten", as proposed by the European Commission, "raises unrealistic and unfair expectations of the proposals" and poses "potentially impossible requirements for data controllers to manage third-party erasure".[7] Similar fears about the effectiveness of

[3] EUR-Lex, access to European Union law, "Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003", http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003R1882:EN:NOT

[4] http://ec.europa.eu/justice/data-protection/minisite/

[5] ibid

[6] EUR-Lex, access to European Union law, "Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL", COM/2012/010 final - 2012/0010 (COD), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012PC0010:en:NOT

[7] The Guardian, "Britain seeks opt-out of new European social media privacy laws", 4th April 2013, http://www.theguardian.com/technology/2013/apr/04/britain-opt-out-right-to-be-forgotten-law

Article 17 have been expressed by other organisations[8] such as the London-based group "Privacy International" and Facebook themselves, especially when personal data have been spread to third parties prior to the exercise of the right to oblivion.

Finally, the issue of privacy in electronic communications is further treated at the EU level via the 2002 Privacy and Electronic Communications Directive[9] of the Telecommunications Package (treated in the next section). The Directive poses additional safeguards on the processing of personal data subject to communications services in areas such as:[10]

- **Processing security** by the communications service provider
- **Confidentiality of communications** which asks Member States to ensure the confidentiality of communications over a public network via legislation
- **Data retention** which poses erasure and anonymisation of data no longer required for the purpose of a communication or billing, with, however, exceptions regarding criminal investigations or national security, defence and public security matters.
- **Unsolicited communications (spamming)**
- **Cookies**
- **Public directories** listing only after consent is given
- **Controls** consisting of a system of legal sanctions for infringements and the establishment of National Regulatory Authorities (NRA).

An in-depth discussion of the privacy-related challenges relevant to the use of social media in emergency situations is included in Chapter 3 of this document.

2.1.2 Telecommunications

European policy on telecommunications relies on the so-called "Telecommunications Package"[11], a set of Directives, Decisions and Regulations aimed at the opening-up of the relevant market to competition in relation to technological developments and the need for stimulating investment.

The main Directive (Framework Directive) is 2002/21/EC[12] plus four other Directives, namely the "Authorisation Directive"[13], the "Access Directive"[14], the "Universal Service Directive"[15] and the "Privacy and Electronic Communications Directive"[16], all dated in 2002.

[8] ibid

[9] Europa, summaries of EU legislation, "Data protection in the electronic communications sector" http://europa.eu/legislation_summaries/information_society/legislative_framework/l24120_en.htm

[10] ibid

[11] Europa, summaries of EU legislation, "Regulatory framework for electronic communications", http://europa.eu/legislation_summaries/information_society/legislative_framework/l24216a_en.htm

[12] EUR-Lex, access to European Union law, "Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002", http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0021:EN:NOT

[13] Europa, summaries of EU legislation, "Authorisation of electronic communications networks and services", http://europa.eu/legislation_summaries/information_society/legislative_framework/l24164_en.htm

[14] Europa, summaries of EU legislation, "Access to electronic communications networks", http://europa.eu/legislation_summaries/information_society/legislative_framework/l24108i_en.htm

[15] Europa, summaries of EU legislation,, "Universal service and users' rights", http://europa.eu/legislation_summaries/information_society/legislative_framework/l24108h_en.htm

[16] Europa, summaries of EU legislation,, "Data protection in the electronic communications sector", http://europa.eu/legislation_summaries/information_society/legislative_framework/l24120_en.htm

This is supplemented by the "Radio Spectrum Decision"[17], the 2009 amendments via the "Better law-making"[18] and the "Citizens' rights"[19] Directives and the Body of European regulators for Electronic Communications[20] (BEREC).

The implications of the telecoms legislation at the European level to social networks lie on their provisions on privacy and on the Internet as a communications medium. As examined in the previous section, in what follows we elaborate on the latter issue. Historically, there were no provisions included in the basic legislative body of the 2002 (Telecoms Package) as regards to the features of an Internet service based on broadband. The important concept of the Universal Service Obligation (USO) included in Article 15 of the 2002 Access Directive (2002/22/EC) appears to have been superseded. Not only does it not apply to mobile communications, but it also does not cover broadband Internet services. A Communication from the Commission[21] in 2008 posed the question of whether the USO "is an appropriate tool to advance broadband development and mobile telephony or whether these services should be left to other Community instruments or to national measures."[22] The debate has yet to be settled at EU level. The 2009 Citizens' Rights Directive (ref. ibid), among others, states that:

- *"...Data connections to the public communications network at a fixed location should be capable of supporting data communications at rates sufficient for access to online services such as those provided via the public Internet..."* and that

- *"...it is not appropriate to mandate a specific data or bit rate at Community level. Flexibility is required to allow Member States to take measures, where necessary, to ensure that a data connection is capable of supporting satisfactory data rates which are sufficient to permit functional Internet access..."*

This constitutes a deviation from the 2002 Universal Service directive, where a limit of 56kbps was explicitly set for a narrowband connection, in favour of shifting the burden to the Member States. Although more flexibility is there, the availability of a minimum bandwidth under all conditions (to cater for periods of stresses caused by crises) is essential if social media are to function as security enhancers for citizens under duress. As COSMIC has already demonstrated[23], the role of social media in crises has, in many cases, been helpful in

[17] Europa, summaries of EU legislation, "Regulatory framework for radio spectrum policy", http://europa.eu/legislation_summaries/information_society/radiofrequencies/l24218a_en.htm

[18] EUR-Lex, access to European Union law, "Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009", http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009L0140:EN:NOT

[19] EUR-Lex, access to European Union law, "Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009", http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009L0136:EN:NOT

[20] Europa, summaries of EU legislation, "The Body of European Regulators for Electronic Communications (BEREC)", http://europa.eu/legislation_summaries/information_society/legislative_framework/si0015_en.htm

[21] Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the second periodic review of the scope of universal service in electronic communications networks and services in accordance with Article 15 of Directive 2002/22/EC (COM (2008) 572 final), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52008DC0572:EN:NOT

[22] http://europa.eu/legislation_summaries/information_society/legislative_framework/l24108h_en.htm

[23] Papadimitriou, A., Yannopoulos, A., Kotsiopoulos, I., Finn, R., Watson, H, Wadhwa, K and Baruh, L., "Case studies of communication media and their use in crisis situations", *Deliverable 2.2 of the COSMIC project,* 30 September 2013.

saving lives. From that point of view, one can argue that a minimum guaranteed bandwidth able to support social networking and other web 2.0 functions throughout the EU, sustainable under adverse conditions (such as those of a crisis), would be desirable.

Policy issue
The lack of an EU-wide imposed minimum bandwidth can have implications on the overall true ability of an internet connection supplied by a Universal Provider to support social network based communication, especially during a crisis.

To serve the general debate and to prepare the road for future amendments, a range of policy options on the general issue of extending a USO to broadband services can be found at a report submitted to the Commission in October 2010.[24]

2.1.3 Towards 2020: the Digital Agenda

Given the previous section, one should not infer that there is no long term policy direction for broadband Internet in Europe. The debate, as shown above, centres on how this can be conducted in a more efficient way. Pillar IV of the Digital Agenda for Europe on "Fast and Ultra-fast Internet Access"[25] states that "to match world leaders like South Korea and Japan, Europe needs download rates of 30 Mbps for all of its citizens and at least 50% of European households subscribing to internet connections above 100 Mbps by 2020." More revealing of the policy intentions is Action 42[26] of the Pillar IV, where the role of public intervention in the deployment of broadband networks is considered crucial in counteracting the "risk that the deployment of fast broadband networks will focus mainly in a few high-density zones leaving rural and remote areas excluded."

Although policy at technical (bandwidth availability) level is important, preservation of the openness of the Internet and of the freedom of citizens to access and run applications and content are becoming increasingly relevant. In fact, this is a consequence of the growth of traffic via the Internet, which has resulted in non-transparent traffic management techniques used by Internet Service Providers (ISPs) and which, in turn, result in Peer-to-Peer (P2P) and VoIP restrictions in fixed and mobile networks. Recognising this threat, Action 115[27] of Pillar IV (Recommendation on safeguarding the open Internet for consumers) calls for EU action to "promote a common regulatory approach among National Regulatory Authorities (NRAs) towards the open Internet and provide a clear and predictable framework for all stakeholders in Europe." Although this does not appear today as a direct threat to social networking (as envisaged in its use during emergencies), use of increased bandwidth for potentially life saving video-streaming activities, for example, may be adversely affected when needed (i.e. during crisis) by traffic management policies of the ISP.

Partial application of the envisaged regulatory framework on the open Internet is also included in the 2009 telecoms Directives (see previous section), according to which

[24] Van Dijk Management Consultants, SVP Advisors, time.lex, "Final Report for the study on the Impact of EU Policy options for revision of the universal service provision", Assignment under the
Framework Contract for Impact Assessment and Evaluation-Related-Services N° 2007/035 – LOT 2, 25 October 2010

[25] http://ec.europa.eu/digital-agenda/en/our-goals/pillar-iv-fast-and-ultra-fast-internet-access

[26] http://ec.europa.eu/digital-agenda/en/pillar-iv-fast-and-ultra-fast-internet-access/action-42-adopt-eu-broadband-communication

[27] http://ec.europa.eu/digital-agenda/en/pillar-iv-fast-and-ultra-fast-internet-access/action-115-recommendation-safeguarding-open-internet

subscribers should be able to access and distribute information or run applications and services of their choice, under transparency and suitable quality of service (QoS) levels across Europe. National Regulatory Authorities (NRAs) are also empowered to safeguard net neutrality.

2.1.4 Other considerations

Social networks, by nature, offer services (not a priori defined) which share arbitrary, unstructured information with specific, selected groups of people. Their main mechanism is forms of authentication, designed to restrict access to previously defined groups. One can legitimately claim that in times of crises wider access of the information any such network contains by, for example, other such networks and possibly emergency services is important, thus the need for interoperability protocols. The difficulties should not be underestimated, however, as personal data leaks can have serious consequences: residence addresses made widely known can result in assaults and burglaries and personal life events can become the object of malicious exploitation. There will be further elaboration on this issue in the second part of this document.

Policy issue
The tradeoffs between privacy and the need for open interoperability standards (at technical and semantic level) for social network data, especially in the case of an emergency, are a challenging issue for technical (protocol design) as well as policy research. This is in view of the trade-off required between wider access to information and the resulting increased risk of malicious exploitation of personal data.

2.2 STANDARDISATION AND SOCIAL MEDIA

This chapter focuses on the technical state of the art in standards that apply to social media, from a crisis management perspective. The evolution of social media is influenced by many, strong and potentially contradictory forces, such as market forces, the common interest, government regulation, and unpredictable scientific and technological innovation. Social media are a relatively new technology, and are still evolving rapidly, thus it is important to consider already-existing standards, gaps where standardisation is missing, as well as current trends with respect to standardisation. In the context of social media the question of standardisation is a complicated and important one, therefore in the present chapter we focus on this topic, since social media are the core concern of the COSMIC project.

2.2.1 Discussion of standardisation of social media in the context of crisis management

The value of standardisation for practical technology is significant across a number of dimensions, including the following[28, 29]:

- Compatibility
    - definition[30]: "*in telecommunications, compatibility is the capability of two or more items or components of equipment or material to exist or function in the same system or environment without mutual interference; in computing,*

[28] Langenberg, T. (2005). "*Standardisation and Expectations*." Berlin: Springer-Verlag.

[29] Murphy, C. N.; Yates, J. (2008). "*The International Organisation for Standardisation (ISO) : Global Governance Through Voluntary Consensus*." New York: Routledge.

[30] http://en.wikipedia.org/wiki/Compatibility

compatibility is the capability that allows the substitution of one subsystem (storage facility), or of one functional unit (e.g., hardware, software), for the originally designated system or functional unit in a relatively transparent manner, without loss of information and without the introduction of errors."

- Interoperability
  - definition[31]: "*interoperability is the ability of making systems and organizations to work together (inter-operate). While the term was initially defined for information technology or systems engineering services to allow for information exchange, a more broad definition takes into account social, political, and organizational factors that impact system to system performance*."
- Commoditisation
  - definition[32]: "*commoditisation is defined as the process by which goods that have economic value and are distinguishable in terms of attributes (uniqueness or brand) end up becoming simple commodities in the eyes of the market or consumers. It is the movement of a market from differentiated to undifferentiated price competition and from monopolistic to perfect competition*."
- Safety
  - definition[33]: "*safety is the state of being "safe", the condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or other types or consequences of failure, damage, error, accidents, harm or any other event which could be considered non-desirable. Safety can also be defined to be the control of recognized hazards to achieve an acceptable level of risk. This can take the form of being protected from the event or from exposure to something that causes health or economical losses. It can include protection of people or of possessions*."
- Quality
  - definition[34]: "*quality in business, engineering and manufacturing has a pragmatic interpretation as the non-inferiority or superiority of something; it is also defined as fitness for purpose. Quality is a perceptual, conditional, and somewhat subjective attribute and may be understood differently by different people. Consumers may focus on the specification quality of a product/service, or how it compares to competitors in the marketplace. Producers might measure the conformance quality, or degree to which the product/service was produced correctly. Support personnel may measure quality in the degree that a product is reliable, maintainable, or sustainable. Simply put, a quality item (an item that has quality) has the ability to perform satisfactorily in service and is suitable for its intended purpose*."
- Repeatability
  - definition[35]: "*repeatability or test-retest reliability is the variation in measurements taken by a single person or instrument on the same item and under the same conditions. A less-than-perfect test-retest reliability causes test-retest variability. Such variability can be caused by, for example, intra-*

[31] http://en.wikipedia.org/wiki/Interoperability

[32] http://en.wikipedia.org/wiki/Commoditization

[33] http://en.wikipedia.org/wiki/Safety

[34] http://en.wikipedia.org/wiki/Quality (business)

[35] http://en.wikipedia.org/wiki/Repeatability

> *individual variability and intra-observer variability. A measurement may be said to be repeatable when this variation is smaller than some agreed limit. Test-retest variability is practically used, for example, in medical monitoring of conditions. In these situations, there is often a predetermined "critical difference", and for differences in monitored values that are smaller than this critical difference, the possibility of pre-test variability as a sole cause of the difference may be considered in addition to, for examples, changes in diseases or treatments*."

Standardisation can be seen by both industry and consumers as offering a trade-off comprising significant advantages as well as significant disadvantages.

- For industry
    - Standardisation is capable of infusing life into a market, helping it to grow. This occurs because standardisation facilitates different companies to bring skills and ideas to the market, improving their internal efficiency and especially the collaboration between companies addressing the same market, and ultimately leading to their better performance and results. Therefore, industry that profits due to the existence of the market should view standardisation as a great opportunity to increase profit.
    - Standardisation is a process of "levelling the playing field" and increasing competition. This is because it lowers the barrier of entry into the market, and allows specialists to contribute to the market, thus breaking an initial monopoly or oligopoly that may have developed under the control of early dominant companies. Therefore, industry that is already in full control of a market, or aiming to gain such control, can view standardisation as a great threat against its opportunity for monopolistic profits.
- For consumers
    - Standardisation supports the development of higher-quality and less-expensive products and services. This occurs because of the efficiency gains and the exploitation of specialist contributions as discussed above. Therefore, consumers should view standardisation as a great opportunity to motivate industry to fairly serve the true needs of the consumers.
    - Standardisation inhibits innovation when it decreases the potential returns that industry expects from developing new and improved products and services. This occurs because companies forced to offer standard products or services cannot innovate so as to differentiate their offerings, adding value for the customer and competing effectively with their competitors – price differentiation becomes the dominant point of competition. Therefore, consumers can view standardisation as a mechanism that suppresses quality in the products and services available to them.

Social media are innovative services, based on state-of-the-art technologies, and are constantly evolving. We can use a distinction applied to the question of standardisation of Cloud Computing by Krechmer[36] to elucidate the social media standardisation question:

- *Standardisation of similarity* is the process of controlling a market so as to enforce similarities between the products and services themselves. Although the benefits described above do apply in this case, standardisation of similarity forces the homogeneity of the

[36] Ken Krechmer, "Cloud computing standardization," in *How does electrotechnology impact economic, social and environmental development? Winning papers from the IEC-IEEE Challenge 2012*, p. 15-25, Geneva, Switzerland.

products and services, thus reducing variation in the market, and thereby reducing innovation. Standardisation of similarity is appropriate for mature markets and technologies, and for dimensions of the products and services where homogeneity is more important than innovation – for example, minimum food quality or the matching characteristics of roads and automobiles.

- *Standardisation of compatibility* is the process of controlling a market so as to enforce different products and services in the market to be usable in conjunction – for example, the Universal Serial Bus allows any computer to be connected to any peripheral device, and it should be noted that the connection technology itself (ports, connectors, wires, controllers) is not a core product in the computing market, but it *is* a core enabler for other products of greater direct value.

It is easy to see that standardisation of similarity in the context of social media is a preposterous idea. It would imply Social Networking Sites being constrained to offer similar services. For example, a Facebook post comprising more than 140 characters is too long to be tweeted on Twitter, so an effort towards standardisation of similarity might call for all posts to be short enough so that they can be shared by users regardless of which Social Networking Site they use to transmit the message. This is clearly an (utterly) undesirable scenario. However, the irrelevance of standardisation of similarity to social media does not imply irrelevance of standardisation in general to social media. Standardisation of compatibility is relevant, practically feasible and capable of generating great value for social media users.

Standardisation of compatibility in the context of social media means that social media as well as other tools, such as data mining tools or content archiving tools, are able to access and use the functions and content of all (other) social media. Very good examples of this capability arise in the context of crisis management:

- Data mining tools accessing tweets transmitted from a disaster area, in order to accurately assess the situation on the ground, e.g. predicting an outbreak of a disease.
- Crisis mapping tools drawing images posted to a photo sharing network from a disaster area, in order to enable the visualisation of the geographic aspects of the disaster, e.g. where the damage is the worst.
- Content aggregation tools, enabling a humanitarian agency to monitor calls for help that are transmitted through any variety of social media.

Standardisation of compatibility can be pursued using the technique of *adaptability standards*, which are *meta standards*[37] enforcing compatibility throughout the evolving lifecycles of the addressed technologies, by explicitly modelling and managing a technology's

- capabilities,
- their versioning,
- a negotiation process between components that allows compatible interfaces to be determined whenever required, and
- the relevant intellectual property rights

While it is acceptable that for-profit companies avoid standardisation of similarity, which would act indefensibly against their interests, the avoidance or boycotting of *adaptability standards* hurts the overall market and aims to lock potential competitors out of that market altogether, therefore it can be morally rejected as a business practice. When companies pursue

[37] K. Krechmer, "Fundamental Nature of Standards", Technical Perspective, *IEEE Communications Magazine*, Vol. 38, #6, June, 2000, p. 70. Adaptability standards are termed etiquettes in this paper.

such a strategy, the result is often a "standards war", more usually termed a "formats war",[38] where competitors each aim to force de facto standards upon the market by achieving their own format's popular adoption, giving the winner power over the market.

Following this discussion, the remainder of this chapter addresses the key areas where standardisation of compatibility can increase the value of social media, especially in the context of crisis management. Since standardisation of similarity is inappropriate, and also not evidenced in the market, there is nothing to document here about standardisation of the core services of social media, such as posting, viewing and searching content through a Social Networking Site's custom user interface. Rather, connectivity and compatibility issues of social media are addressed. Specifically, we consider:

- standardisation of telecommunications technology underlying social media
- standardisation of the delivery and presentation layers of social media
- standardisation of social media data
- standardisation of technical means for interacting with social media services

The first two of these standardisation challenges are, largely, already-solved issues, while the last two of these standardisation challenges are, largely, unsolved issues. It is interesting to consider them together, as this illustrates the gradual progress of social media standardisation.

2.2.2 Standardisation of telecommunications technology underlying social media

Telecommunications have been the subject of standardisation since at least 1865[39]. As discussed in D1.2 of COSMIC, telecommunication technologies are highly mature, highly standardised, and offer a well defined technological layer for data transmission over which social media can be built. Newer telecommunication technologies periodically appear and provide new capabilities, such as mobility, but applications exploiting them can remain agnostic to the technical details of the data transmission process and rely on standardised abstractions of this transmission capability, such as messages, connections etc. In our discussion on policy issues in this document, we also discuss the European regulatory framework for electronic communications[40], which, it should be noted, regulates standards aimed at organising and perpetuating these conditions.

2.2.3 Standardisation of the delivery and presentation layers of social media

Social Media are delivered either as web pages or through mobile apps. Mobile apps primarily target smartphones and exploit the devices' capabilities to the maximum, whereas delivering social media through mobile web browsers benefits from standardisation; this dilemma, weighing customisation versus standardisation, remains unresolved and the subject of debate[41], yet in the long term the balance seems to be tipping in favour of standardisation[42]: HTML5, despite its not yet being finalised, allows major benefits such as "build once, deploy to many" (as opposed to the need to implement a separate app for each platform, such as different mobile operating systems, but also different smart TV solutions, different in-vehicle entertainment systems, etc) and better searchability.

[38] http://www.switched.com/2010/09/24/format-wars-a-history-of-what-could-have-been-from-betamax-to

[39] http://www.itu.int/en/history/Pages/Home.aspx

[40] http://europa.eu/legislation_summaries/information_society/legislative_framework/l24216a_en.htm

[41] http://www.theguardian.com/media-network/media-network-blog/2013/feb/07/html5-native-apple-android-strategy

[42] http://www.wired.com/insights/2013/09/auto-industry-to-rev-up-the-death-of-native-apps-rise-of-html5

Web standardisation has a long and uneven history[43,44], but, ultimately, globally accepted and almost universally implemented, largely consensual, de jure standards have prevailed[45]. Developers can confidently rely on a broad variety of standards for the delivery and presentation[46] of the social media products on offer, including:

- (X)HTML, CSS, DOM, XForms, SVG, RDF, GRDDL, OWL[47]
- HTML5, Microdata, Web Applications, Web Forms, Web Workers[48]
- Unicode Standard, Unicode Technical Reports (UTRs)[49]
- Web site engineering and other IT standards, for example, user interface standards, PNG functional specification[50]
- ECMAScript[51]
- Domain names, IP address coordination, protocol assignments[52]
- Internet standard (STD) documents, Request for Comments (RFC) documents, for example, proper use of HTTP, MIME, and URI[53]
- Dublin Core Metadata[54]

2.2.4 Standardisation of social media data

Social media data is intrinsically inter-referenced, since the handling of relationships is the main differentiator between social networking services and the older Web; often, the entities whose relationships are defined in social media data are real-world entities, such as people. Additionally, social media data is vast: billions of users are generating data on a regular basis. Finally, social media data is rich in semantics and in digital media content, encompassing structured and semi-structured representations of a variety of human relationships[55] as well as digital media content such as images and videos.

A useful representation of social media data will effectively deal with these characteristics. It will be able to explicitly identify or define the entities it refers to, and represent the relationships between them. It will be amenable to efficient, automated processing by computers, as no human user is capable of manually examining all the social media data being produced. Finally, it will be compatible with a modelling mechanism capable of capturing the rich semantics of the data.

[43] http://www.w3.org/Consortium/facts.html#history

[44] http://www.webstandards.org

[45] Sikos, Leslie. "*Web standards: mastering HTML5, CSS3, and XML.*" Apress, 2011.

[46] It should be noted that delivery includes the conceptual structure of the content, which includes the structured markup and the semantic markup of the content – both underlying the final presentation features which determine the visual characteristics of the content

[47] www.w3.org

[48] www.whatwg.org

[49] www.unicode.org

[50] www.iso.org

[51] www.ecmainternational.org

[52] www.iana.org

[53] www.ietf.org

[54] www.dublincore.org

[55] When one user "Likes" another, this is an explicit assertion of a positive response of the first user towards the second. However, if one user tags another in a photograph, this provides implicit evidence that the first user recognises the second visually. There are very many such items of relationship information to be accessed or discovered in social media data.

Linked Data provides a standardised way to represent data, which is highly appropriate to social media data. Linked Data[56] "*refers to data published on the Web in such a way that (i) it is machine-readable, (ii) its meaning is explicitly defined, (iii) it is linked to other external data sets, and (iv) can in turn be linked to from external data sets. Linked Data requires the identification of entities with URI references that can be dereferenced over the HTTP protocol into a common semantic data model, such as RDF. The use of Linked Data is advantageous as it inherently facilitates interoperability and integration of data from disparate data sources. It also opens up possibilities for carrying out inference and analytics over the data.*"

Although Linked Data is an excellent representation mechanism for social media data, as a generic framework it is agnostic to the specific semantics of social media data. Therefore, Linked Data standardises a structural representation mechanism that is appropriate for social media data, but not a semantic model of social media data.

In order to represent the internal semantics of social media data, a semantic model, or at least a descriptive data or object schema, is required. A complete semantic model of all social media data would be a very powerful tool, however so far no such model is available. Indeed, any such semantic model would need to be aggressively maintained, since social media themselves, together with their underlying data, are still evolving quite rapidly. Various solutions exist which partially meet these requirements, such as:

- FOAF ontology[57]
  - definition: "*this ontology is used to describe people and social relationships on the Web. It is mostly focused on people's existence in the virtual world, with many properties related to online activity or identity: foaf:mbox, foaf:skypeID, foaf:msnID, foaf:geekcode, etc. Other concepts, such as family relations, physical address, etc, are not modelled. It provides similar information on organisations or groups with a similar focus on their existence on the Web (work place webpage, etc). It is particularly well suited for describing people on Web-based Social platforms (facebook, twitter, blogspot, etc).*"
- SIOC ontology[58]
  - definition: "*this ontology is used to describe online communities such as forums, blogs, mailing lists, wikis. It complements FOAF by focusing on the description of the products of those communities: posts, replies, threads, etc.*"
- OpenSocial Data Specification[59]
  - The OpenSocial Data Specification defines all the data objects used in the OpenSocial APIs. OpenSocial is discussed in more details in the following sub-section.
- The SocIoS Object Model and the SocIoS Ontology[60]
  - definition: The SocIoS Object Model is at the core of the European project SocIoS, and supports consistent operations (the SocIoS Core Services) to be performed on social media data, regardless of the Social Networking (SN) Site from which the data is drawn. *"The Object Model and the Core Services constrain the datatypes and the services that SocIoS Auxiliary Services can use*

[56] Bizer, C., 2009. The Emerging Web of Linked Data. *Intelligent Systems*, 24(5), pp.87–92.

[57] http://www.foaf-project.org

[58] http://sioc-project.org

[59] http://opensocial.github.io/spec/2.5.1/Core-Data.xml and http://opensocial.github.io/spec/2.5.1/Social-Data.xml

[60] http://www.sociosproject.eu/Dissemination/Deliverables/tabid/119/language/en-GB/Default.aspx

for their operation. SocIoS object model is a close variation of OpenSocial Data Specification, as developed by Google along with MySpace and a number of other social networks. The Object Model defines five core concepts that are directly mapped to entities that live in the underlying social networks. The core concepts are: Person, MediaItem, Activity, Message and Group and are used to represent SN users, SN content, SN activities, short messages posted to SN users and groups of users, respectively."

  - definition: the SocIoS Ontology *"captures the result of the conceptualization of the SocIoS domain as part of the process to define the SocIoS Object Model. The objective is to semantically describe the elements of the SocIoS object model."*

2.2.5 Standardisation of technical means for interacting with social media services

In this sub-section, we describe a whole stack of technologies for interacting with social media services[61]. We cover an open source technology stack, which provides a reasonable basis for a standardisation of tools for interacting with social media services. The negative side of this choice is that some of the technologies described have not been adopted by Facebook and Twitter – for example, OpenSocial. These social media "majors" often use proprietary standards that only work with their own services (although their precise practices fluctuate over time). We have a clear example of market leaders trying to lock potential competitors out of the market by avoiding standardisation, as discussed in the beginning of this chapter. On the other hand, it can also be argued that the open standards are being promoted by Facebook and Twitter competitors who would use such standards as a wedge to let themselves into a business created by Facebook and Twitter and largely ignored by them until too late – these competitors include Google, Yahoo! and IBM. While the open standards are definitely the preferable solution in general, the motivations of companies for supporting them or avoiding them are thus quite complicated and not trivial to judge morally.

The major set of open source technologies specifications include:

- OpenSocial[62]
  - definition: OpenSocial supports exploring the social graph and application development for social media applications. "*OpenSocial is a public specification that defines a component hosting environment (container) and a set of common application programming interfaces (APIs) for web-based applications. It can be used as a general-use runtime environment for allowing untrusted and partially trusted components from third parties to run in an existing web application. OpenSocial is the most mature standards-based component model for cloud based social apps. Using OpenSocial, it is easy to develop an app that reaches users in their activity stream, in content, in email, or even on their mobile device."*
- Shindig[63]
  - definition*:* Apache Shindig is a *container implementation* for OpenSocial. It is a framework for web-based applications. It provides a reference implementation for the OpenSocial standard, covering both the server-side and

[61] following the organisation of material in: LeBlanc, Jonathan. *Programming Social Applications: Building Viral Experiences with OpenSocial, OAuth, OpenID, and Distributed Web Frameworks*. O'Reilly Media, Inc., 2011.

[62] http://opensocial.org

[63] http://shindig.apache.org

the client-side. It addresses the rendering of OpenSocial gadgets inside the web browser. Its goal is to enable the very easy and fast implementation work required for sites to host social apps.

- OAuth[64]
  - definition*:* OAuth is an open standard, defining an open authentication protocol. *"It allows secure authorization in a simple and standard method from web, mobile and desktop applications. OAuth is an open standard for authorization. OAuth provides a method for clients to access server resources on behalf of a resource owner (such as a different client or an end-user). It also provides a process for end-users to authorize third-party access to their server resources without sharing their credentials (typically, a username and password pair), using user-agent redirections."*
- OpenID[65]
  - definition: "*OpenID is an open standard that allows users to be authenticated by certain co-operating sites (known as Relying Parties or RP) using a third party service, eliminating the need for webmasters to provide their own ad hoc systems and allowing users to consolidate their digital identities. Users may create accounts with their preferred OpenID identity providers, and then use those accounts as the basis for signing on to any website which accepts OpenID authentication. The OpenID standard provides a framework for the communication that must take place between the identity provider and the OpenID acceptor (the "relying party")."*
- Caja[66] and ADsafe[67]
  - definition: These are tools enabling the safe execution of frontend code. For example, ads executing code in the end user's browser can be made safe using these tools, so that ads can be trusted to promote products or services to users, without fear of introducing malware or having other adverse effects on the user's computer.
- The Open Graph protocol[68]
  - definition: the Open Graph protocol supports the *exploration* of social web entities. "*The Open Graph protocol enables any web page to become a rich object in a social graph. For instance, this is used on Facebook to allow any web page to have the same functionality as any other object on Facebook. While many different technologies and schemas exist and could be combined together, there isn't a single technology which provides enough information to richly represent any web page within the social graph. The Open Graph protocol builds on these existing technologies and gives developers one thing to implement."*
- Activity Streams[69]
  - definition: "*Activity Streams is a foundation for delivering activity content. Activity Streams is an open format specification for activity stream protocols, which are used to syndicate activities taken in social web applications and services, similar to those in Facebook's Newsfeed, FriendFeed, the Movable*

[64] http://oauth.net/

[65] http://openid.net

[66] http://code.google.com/p/google-caja

[67] http://www.adsafe.org

[68] http://ogp.me

[69] http://activitystrea.ms

Type Action Streams plugin, etc. An activity stream is a list of recent activities performed by an individual, typically on a single website."

- WebFinger[70]
    - definition: "*WebFinger is a means of discovering public user data using email addresses. WebFinger is a protocol that allows for discovery of information about people and things identified by a URI.*"
- OExchange[71]
    - definition: "*OExchange an open protocol for sharing any URL with any service on the Web.*"
- PubSubHubbub[72]
    - definition: "*PubSubHubbub is a means of syndicating user conversations from a root provider to multiple subscribers. PubSubHubbub is a simple, open, server-to-server webhook-based pubsub (publish/subscribe) protocol for any web accessible resources. Parties (servers) speaking the PubSubHubbub protocol can get near-instant notifications (via webhook callbacks) when a topic (resource URL) they're interested in is updated.*"
- The Salmon protocol[73]
    - definition: "*The Salmon protocol is a message exchange taking the foundation of PubSubHubbub and unifying conversations between publishers and subscribers. It is a protocol running over HTTP designed to decentralize commentary and annotations made against newsfeed articles such as blog posts. It allows a single discussion thread to be established between the article's origin and any feed reader or "aggregator" which is subscribing to the content. Put simply, that if an article appeared on 3 sites A (the source), B and C (the aggregates), that members of all 3 sites could see and contribute to a single thread of conversation regardless of site they were viewing from.*"

2.2.6 In the news: towards Social Standards – W3C and OpenSocial Foundation collaborating

A current development is that W3C is now coordinating with the OpenSocial Foundation in order to produce standards directly focusing on social media. A workshop on this topic was held in San Francisco, on the 7th and 8th of August 2013[74], and the workshop's report[75] was published as this document was being written.

The objective of the collaboration is to "make social a first-class citizen of the Web", by developing open, royalty-free standards and patents under the respected W3C brand, ensuring the quality and interoperability of social media services, applications and data, and promoting competition in the social media industry to focus on the innovation and value of services provided, rather than in customer lock-in. An emphasis is placed on reliability and availability, focusing on the business potential of social media; however these properties are also critical for crisis management, since unreliable or unevenly available communications tools during a crisis are a serious problem.

[70] http://code.google.com/p/webfinger
[71] http://www.oexchange.org
[72] http://code.google.com/p/pubsubhubbub
[73] http://www.salmon-protocol.org
[74] http://www.w3.org/2013/socialweb
[75] http://www.w3.org/2013/socialweb/report

Currently, strategy is still being decided upon, Working Groups are being formed, and concrete technologies are being assessed. This means, there is not as yet a concrete, immediately usable output available from this activity. However, should the intended progress towards Social Standards be achieved, the positive impact on crisis management can be considerable.

2.3 CONCLUSION

In this chapter, existing policies, standards and opportunities relating to social media and crises were identified. Applicable legislative measures taken at EU level cover the areas of privacy, data protection and telecommunications. The partners highlighted the relevance of the reform of the current Data Protection Directive (1992), proposed by the European Commission, and, in particular, its provision for added protection of online data via the "right to oblivion" (Article 17). On the telecommunications side, the implications of the, as yet unsettled, issue of the lack of an EU-wide imposed minimum bandwidth obligation on a Universal Provider were noted as a pending policy issue potentially affecting social network based communication, especially during a crisis.

The question of standardisation in social media was found to affect aspects such as compatibility, interoperability, safety and quality both from the point of view of the industry as well as consumers. The partners examined standardisation challenges such as the underlying telecommunications technologies, the presentation layer of social media, the data involved and the means of interacting with social media services. For the semantics-rich social media data, representation mechanisms such as Linked Data were identified and commented upon, along with various emerging attempts for describing semantic models. Finally, examination of the developing and varied landscape of tools for interacting with social media services revealed the complex interplay between market leaders and their competitors and correspondingly between proprietary and open standards.

3 CHALLENGES POSED BY PRIVACY AND SECURITY

There are a number of inherent challenges to be taken into consideration if those involved in crisis management activities are to optimally utilise emerging technologies as part of their efforts in preparing for and responding to crises involving the security of citizens. In part, Task 3.2 of the COSMIC project involves examining the political, social and industrial implications of the use of emerging technologies in crisis situations. Accordingly, this chapter, a preliminary activity in Task 3.2, seeks to examine those challenges relating to privacy and security issues concerning the use of social media in emergency management activities. Such privacy related challenges include: conforming to EU policy, being transparent, and issues surrounding data protection, surveillance and anonymity. Additionally, this chapter will also (briefly) discuss security related challenges, including: the protection, reliability and accuracy of information and the risk of vigilante justice.

In order to briefly examine these privacy and security challenges, partners have conducted desk-based research to further explore relevant literature including news articles (including blog posts), industry reports and peer-reviewed journal articles relating to some of the privacy and security challenges that are relevant to the use of social media in emergency situations.

3.1 PRIVACY

As extensively discussed and scrutinised within policy, the press and the academic arena, privacy often appears as a key concern in relation to new and emerging technologies, including social media.[76] The concept "privacy" is notoriously difficult to define. Solove argues that privacy is best understood as a "family of different yet related things".[77] In 1997, Roger Clarke outlined a taxonomy of four different types of privacy: privacy of the person, privacy of personal data, privacy of personal behaviour and privacy of personal communication.[78] More than a decade later, Finn, Wright and Friedewald updated Clarke's categories to include three additional types of privacy including; privacy of thoughts and feelings, privacy of location and space and privacy of association (including group privacy).[79] Such privacy considerations are relevant, particularly when considering the use of social media by stakeholders, including members of the public, in various types of crisis situations. Accordingly, with an increasing emphasis being placed on the use of social media for different stages of emergency management, it is necessary for stakeholders to consider the many privacy related challenges that they may need to confront, particularly: relevant EU policy, principles relating to data protection, anonymity and other privacy related considerations, particularly in relation to surveillance.

3.1.1 EU Policy

One of the most prominent privacy related issue to consider in relation to engagement with social media, as a tool for crisis management activities is the issue of ensuring that a person's

[76] Watson, H., and Finn, R.L., "Privacy and ethical implications of the use of social media during a volcanic eruption: some initial thoughts", *Proceedings of the 10th International ISCRAM Conference*, Baden-Baden, Germany, May 2013.
[77] Solove, Daniel J., *Understanding Privacy*, Harvard University Press, Cambridge MA and London, 2008. [p. 9]
[78] Clarke, Roger, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms", Xamax Consultancy, Aug 1997. http://www.rogerclarke.com/DV/Intro.html
[79] Finn, Rachel L., David Wright, and Michael Friedewald, "Seven types of privacy", in Serge Gutwirth, Yves Poullet et al. (eds.), *European Data Protection: Coming of Age*, Springer, Dordrecht, 2013 [forthcoming].

privacy of data and image is not affected. As discussed in Chapter 2 of this report, ensuring adequate data protection measures is of the utmost concern to the EU, as indicated by Article 8 "Protection of personal data" within the Charter of Fundamental Rights of the European Union (2000/C 364/01); "everyone has a right to the protection of personal data".[80] This is also evidenced via the current legal framework, the 1995 Data Protection Directive (95/46/EC). At the core of this Directive is the "effective protection of the fundamental right of individuals to data protection".[81] As argued by King and Jessen, the Directive has eight key principles:[82]

> "Pursuant to the Data Protection Directive, personal data may only be collected for specified, explicit and legitimate purposes and may not be processed inconsistently with those purposes (the "finality principle"). The purpose of the processing itself must be legitimate (legitimacy principle), and the data subject must be fully informed on the details of the processing, including who has access to the data, how it is stored and how the subject can review it (transparency principle). The "proportionality principle" requires that personal data be adequate, relevant and not excessive in relation to the purposes for which it is collected and further processed. Sensitive data receives heightened data protection."

However, as the framework is somewhat dated, it does not adequately consider important developments since 1995, including the ever-expanding impact of globalisation and enhanced technologies that surpass global boundaries, such as social networking websites. Consequently, on the 25 January 2012 the EU released a draft version of a reform to its data protection policy; a "General Data Protection Regulation" (GDPR).[83] Ultimately the "new" Directive would "strengthen online privacy rights and boost Europe's digital economy".[84] Proposed changes focus on:

> "reinforcing individuals' rights, strengthening the EU internal market, ensuring a high level of data protection in all areas (including police and criminal justice cooperation) ensuring proper enforcement of the rules, facilitating international transfers of personal data and setting global data protection standards. The proposed changes will give people more control over their personal data and make it easier to access it. They are designed to make sure that people's personal information is protected – no matter where it is sent, processed or stored – even outside the EU, as may often be the case on the Internet".[85]

More specifically and relevant to the collection of personal data within crisis management, the GDPR has strengthened its position on consent to say that it needs to be "explicit" (Art. 4 (8)). Furthermore, Art 55. of the GDPR provides for derogations, for instance in case of informed consent, on "important grounds of public interest", and for the purpose of legitimate interests which "cannot be qualified as frequent or massive").", implying that consent can be undermined

[80] "Chart of fundamental rights of the European Union", *Official Journal of the European Communities, 2000/C 364/01,* 18 December 2000. http://www.europarl.europa.eu/charter/pdf/text_en.pdf

[81] "Why do we need an EU data protection reform?", *European Commission,* 2012. http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf

[82] King, N.J. and Jessen, P. W., "Profiling the mobile customer e Privacy concerns when behavioural advertisers target mobile phones - Part I", *Computer, law and security review,* Vol. 26, 2010, pp. 455-478. [p. 464]

[83] "REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", *European Commission,* COM(2012) 11 final, 25 January 2012.

[84] "Commission proposes a comprehensive reform of the data protection rules", *European Commission, Justice, Data protection, Newsroom,* 25 January 2012. http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

[85] "Data protection reform: Frequently asked questions", *European Commission MEMO/12/41*, 25 January 2012. http://europa.eu/rapid/press-release_MEMO-12-41_en.htm?locale=en

for situations such as crises.[86] Another notable point of interest is the clarification of the position on the principle of "data minimisation" (Art 5.).

The intended amendments to the EU framework should be considered by those participating in the use of social media for crisis management within the EU as well as those outside, as this (future) Directive will impact stakeholders across the globe. Such a sentiment is emphasised by the International Committee of the Red Cross (ICRC) in their guidance document for humanitarian and human rights actors; "Professional standards for Protection Work", where they argue that "Protection actors must collect and handle information containing personal details in accordance with the rules and principles of international law and other relevant regional or national laws on individual data protection".[87] Legality issues aside, let us consider the challenges of transparency, proportionality and legitimate purposes, which have important implications for data protection, as well as other privacy, related challenges within the use of new media applications, including social media, in crisis management activities.

Transparency

A key privacy related principle is that of transparency. Generally speaking the term transparency refers to something that is easy to see through, it is clear and explicit. In relation to privacy issues such as data protection, transparency is fundamental to the various activities involved in using social media in crisis management. For instance, there is a need for transparency when requesting information from the public via a social networking site such as Twitter. As revealed in D2.2 of the COSMIC project, following events such as the 2013 Boston attacks, it may be that police require information from the public for investigative purposes. Similarly following a natural disaster such as witnessed following Hurricane Sandy in 2012, in their attempts to respond to social media messages, the New York Fire Department made requests for further information.[88] Accordingly, when requesting information from the public it is necessary for authorities to ensure that they inform those engaging with them via social networking websites what their policies are in relation to ensuring the protection of their data as well as any other intended secondary uses of material. As identified in their protocol, the ICRC argue that:

> "Protection actors must integrate the notion of informed consent when calling upon the general public, or members of a community, to spontaneously send them information through SMS, an open Internet platform, or any other means of communication, or when using information already available on the Internet."[89]

Furthermore, the ICRC recommend that stakeholders should "…establish formal procedures on the information handling process, from collection to exchange and archiving or destruction".[90] Thus ensuring transparency via the inclusion of publicly available data

[86] Hornung, G. "A General Data Protection Regulation for Europe? Light and shade in the Commission's draft of 25 January 2012". *SCRIPTed*, Vol. 9, No. 1, 2012, pp. 64–81. [p. 70]

[87] ICRC, "Professional standards for Protection Work ICRC: carried out by humanitarian and human rights actors in armed conflict and other situations of violence", *International Committee of the Red Cross*, Geneva, Switzerland, 2013. [p. 85].

[88] Papadimitriou, A., Yannopoulos, A., Kotsiopoulos, I., Finn, R., Watson, H, Wadhwa, K and Baruh, L., "Case studies of communication media and their use in crisis situations", *Deliverable 2.2 of the COSMIC project,* 30 September 2013.

[89] ICRC, p. 95.

[90] ICRC, p. 100.

handling policies is an ethical and legal requirement for stakeholders engaging with social media as part of their crisis management activities.

Those organisations that utilise their own blog-based form of communication, where visitors may be able to respond to posts with comments, should also be transparent in their (potential) subsequent use of information they may receive. [91] In addition, they should also be transparent about any policies (e.g., participation rules) they may have relating to monitoring and editorial actions relevant to participation areas on their sites. [92] To illustrate, the American Red Cross have the following, "lawyer-approved" comment policy:

> "Remember, we encourage you to participate in this blog via comments. All viewpoints are welcome, but please be constructive. We reserve the right to make editorial decisions regarding submitted comments, including but not limited to removal of comments. The comments are moderated, so you may have to be a tiny bit patient in waiting to see them. We will review and post them as promptly as possible during regular business hours (Monday through Friday, 8:30 - 5:30)."

As part of organisation's efforts to be transparent and ethical in their activities involving the use of social media prior to, during and after a crisis, it is essential that organisations pay attention to copyright issues. Copyright involves, the legal protection of any medium via its originator, e.g., the copyright of a photograph, website, report, video etc.[93] As argued by Rive et al., it is essential that organisations avoid breaching copyright, and accordingly, when passing on information via a social media application such as Facebook or Twitter, they should ensure they provide some form of citation to demonstrate where the information they are sharing comes from. As recommended by Rive et al., being transparent in the sharing rather than copying of information is crucial, and is one legal means with which breaches of copyright can be avoided.[94] Similarly, for an organisation sharing their own material, it may be advisable[95] for them to place their own work under a copyright license such as a creative commons license, which gives "everyone from individual creators to large companies and institutions a simple, standardized way to grant copyright permissions to their creative work".[96]

Proportionality & legitimate purpose

As identified by Jones and Tahri in their review of EU data protection rules on use of data collected online, the principle of proportionality in relation to online content refers to website operators avoiding "processing excessive, irrelevant or inadequate personal data (given the purposes for which the data were collected and are used".[97] The purpose of this data minimisation principle is to ensure that only the minimum amount of data required is collected. Proportionality is also linked to transparency, in that operators should ensure they inform users if they are to utilise personal data for anything other than what the data was

[91] Rive, G., Hare, J., Thomas, J. and Nankivell, K. "Social Media in an Emergency: A Best Practice Guide", Wellington Region CDEM Group: Wellington, 2012. http://www.gw.govt.nz/assets/Emergencies--Hazards/WREMO/Publications/Social-media-in-an-emergency-A-best-practice-guide-2012.pdf [p. 20]

[92] Rive, G., Hare, J., Thomas, J. and Nankivell, K. "Social Media in an Emergency: A Best Practice Guide", Wellington Region CDEM Group: Wellington, 2012. http://www.gw.govt.nz/assets/Emergencies--Hazards/WREMO/Publications/Social-media-in-an-emergency-A-best-practice-guide-2012.pdf [p. 20]

[93] "Copyright", *Intellectual Property Office,* 30 November 2008. http://www.ipo.gov.uk/copy.htm

[94] Rive et al., 2012, p. 19.

[95] Rive et al., 2012, p. 19.

[96] "Creative commons: about the licenses", *Creative Commons,* no date. http://creativecommons.org/licenses/

[97] Jones, R. and Tahri, D., "An overview of EU data protection rules on use of data collected online", *Computer law & security review,* Vol. 27, 2011, pp. 630-636. [p. 633]

initially collected for.[98] When consent is not able to be collected, data controllers must rely on "legitimate interests", which can be used in some EU Member States to justify data processing.[99]

The consideration of data protection principles such as transparency, proportionality and legitimate purpose are extensive challenges to be acknowledged and responded to by those engaging with the use of social media as part of their crisis management activities. As argued by Palen et al. it is necessary for researchers and stakeholders directly involved in utilising ICT for crisis response purposes to consider how their practices lie within the laws, policies and regulations.[100]

As examined in Chapter 2, there are other important EU policies that should be taken into consideration in relation to the use of new media applications to support crisis management efforts. For now, let us consider more generally what data protection implies for crisis management.

3.1.2 Data protection

Ensuring the adequate protection of data collected or received from others is a crucial challenge that affects all stakeholders involved in utilising social media as part of their crisis management activities. Within the EU (including all countries of the European Economic Areas – EEA, as well as Iceland, Liechtenstein and Norway), data protection involves the adequate protection and use of an individual's personal data. For instance, under the current EU Directive 95/46/EC of the European Parliament and of the Council 1995: under Art. 6 "Principles relating to data quality" data collection must be done so in a manner that data is processed legally and fairly, collected for specific reasons and stored in such a way that it permits the identification of the data subject for no longer than is necessary etc. Furthermore, Art. 10 "Information to be given to the data subject", states that, for instance, the collection of data is under strict conditions and that as part of the collection of data, individuals must be informed about the collection of, and intended use of their data. Art. 12 outlines the individual's rights to access their data. Elsewhere, Art. 17 states that an individual's personal data is protected from misuse and unauthorised disclosure or access.[101] These, and more Articles, set out the parameters with which European's data should lawfully be protected.

When taking this regulation into consideration for crisis management activities involving the collection of data, it is therefore necessary to consider the legal implications of data mining activities. Furthermore, there is a need for the consideration of other national privacy related laws that may impact the use of systems to alert individuals. For instance, in 2009, Federal privacy laws in Australia restricted private (telephone) numbers from being accessed by emergency services. Consequently, following deadly wildfires in Victoria, Australia in February 2009 where 181 people were killed, thousands of people were left unprepared as

[98] Jones and Tahri, 2011, p. 633.
[99] Jones and Tahri, 2011, p. 632.
[100] Palen, L., Anderson, K . M., Mark, G., Martin, J., Sicker, D., Palmer, M and Grunwald, D., "A Vision for Technology-mediated Support for Public Participation & Assistance in Mass Emergencies & Disasters." *Proceedings of the 2010 ACM-BCS Visions of Computer Science Conference*, ACM-BCS, 2010, Swinton, UK, pp. 1-12. http://dl.acm.org/citation.cfm?id=1811182.1811194
[101] "DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data", *Official Journal, L 281* , 23 November 1995. *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML*

officials were still trying to deal with the challenges imposed on them by privacy laws, which restricted them from installing a nationwide fire alert telephone system. [102]

Accordingly, considering the various legal restrictions and requirements and ensuring the adequate data protection policies are implemented as part of an organisations collection and re-use of data is an important and complex challenge to be met. Examples in data protection practices can be seen in the recommendations of the ICRC, who assert that: "Protection actors setting up systematic information collection through the Internet or other media must analyse the different potential risks linked to the collection, sharing or public display of the information and adapt the way they collect, manage and publicly release the information accordingly".[103]

Whilst data protection appears to be a concern for some larger organisations involved in the use of social media as part of their work, this is not always the case. For instance, following the Joplin tornado in 2011, Williams et al. were successful in utilising social media, particularly the Facebook page "Joplin Tornado Info" for search and rescue efforts, and have since published a guide for others to use in implementing their own strategy in the optimum use of social media in crisis management. This guide provides useful information relating to best practices and tools to be used (for instance), but does not include any discussion or mention of privacy or data protection considerations. [104]

There are some groups whom are developing tools and technologies to help provide users with some control (in addition to privacy settings) over the availability of the information they share via their social networking sites. For instance Meier and PopRock Fellows (PopTech & Rockefeller Foundation) are currently considering the use of a no share principle with regards to the posting of tweets to help promote ethical community resilience to crises. The idea of the no share principle is for users to use a hashtag; #noshare or #ns with any material they share in a crisis so as to label it as being something they wish not to be collected, thus promoting a "new norm: avoid it being the right to be social without being sensed or exploited without our knowledge or consent".[105] Meier also refers to the use of tools such as TwitterSpirit and Efemr to reduce the amount of time a tweet will be made publicly available, which could be particularly useful to the protection of sensitive data by providing users with some control over their data.[106]

Integrating privacy considerations into the forefront of the design and subsequent use of new media applications, including social media for crisis management purposes may benefit from employing the principle "privacy by Design" (PbD) which is considered by the European Data Protection Supervisor, Peter Hustinx as an essential principle for enhancing citizen's trust of ICT, where trust and privacy are interlinked.[107] Simply put, as coined in the mid-

[102] "Police detain 2 about wildfires", *The Associate Press, The Jakarta Post,* 12 February 2009. http://www.thejakartapost.com/news/2009/02/12/australian-police-detain-2-about-wildfires.html

[103] ICRC, p. 86.

[104] Williams, R., Williams, G. and Burton, G. "The Use of Social Media for Disaster Recovery", *University of Missouri Extension,* 24 May 2013. [p. 20]

[105] Meier, P., "#NoShare: A Personal Twist on Data Privacy", *iRevolution blog,* 15 September 2013. http://irevolution.net/2013/09/15/noshare-hashtag/

[106] Meier, P., "Data Protection: This Tweet Will Self-Destruct In…", *iRevolution blog,* 6 September 2013. http://irevolution.net/2013/09/06/this-tweet-will-self-destruct/

[107] Cavoukian, Ann., "Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era", in Yee, George O.M., ed. *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards*. IGI Global, 2011pp. 170-208.

nineties by Ann Cavoukian, the Information and Privacy Commissioner of Ontario, Canada, PbD involves "the philosophy and approach of embedding privacy directly into the design and operating specifications of information technologies and systems".[108] Such a philosophy involves a series of considerations, but crucially, those systematically implementing PbD must recognise the "value and benefits of adopting good privacy practices".[109]

Data protection challenges are also present for those commercial organisations that may wish to re-use data they obtain via social networking websites in the aftermath of their interaction with others. For instance, as examined by Watson and Finn, the use of Twitter by some airlines following the travel chaos caused by the eruption of the Eyjafjallajokull volcano in 2010 caused potential data protection and privacy concerns particularly with regards to the profiling of customers:

> "Companies such as Qantas use their social media platform to collect and use personal information about consumers to create user profiles and carry out advertising in the future (Andrejevic, 2012). Second, those relying on Twitter, Facebook or other social media feeds to gather information or solve problems may have had little opportunity to refuse consent for these types of information collection practices without putting themselves at an information disadvantage within a situation in which this information is both reliable and essential. This is indicative of a gradual undermining of consumer consent through the removal of meaningful alternatives, particularly when users are in a vulnerable situation such as in a crisis."[110]

As argued by King and Jessen, behavioural advertising techniques include the use of profiling to produce "targeted advertising to consumers".[111] The extensive use of the web for browsing and shopping, combined with the use of location tracking technologies (such as that included in mobile phones) makes consumer profiling that much simpler, which subsequently have implications for data protection.[112,113] When bringing this back to crisis management, it is essential that those *other* groups involved in responding to a crisis (e.g., critical infrastructure providers) take steps to ensure that those they interact with are aware of their commercial data policies, including the use of customer data for industry purposes.

As briefly examined in this sub-section, it is essential that stakeholders consider the various data protection and privacy implications of their interactions and collection of data from others in the event of a crisis.

3.1.3 Anonymity

An important privacy related consideration with regards to the use of social media in crisis management is upholding the ethical principle of maintaining an individual's anonymity. As argued by Rive et al. it is essential that those organisations involved in sharing material such as photos of disaster sites, take the appropriate measures to ensure the privacy of the public is

[108] Cavoukian, 2011, p. 173.

[109] Cavoukian, 2011, p. 173. [Note: further information relating to the principles of privacy by design including the need for privacy enhancing technologies can be found in the full chapter by Cavoukian].

[110] Watson and Finn, 2013, p. 4.

[111] King and Jessen, 2010.

[112] Ibid.

[113] The proposed update to the EU Data Protection Directive indicates that individuals have a right not to be subject to decisions based on profiling (Art. 20).
"REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", *European Commission,* COM(2012) 11 final¸25 January 2012.

upheld (e.g., masking faces and vehicle number plates).[114] Furthermore, as suggested by the American Red Cross, it is essential that appropriate permission is gained from people/clients to ensure their privacy is respected.[115]

The issue of remaining anonymous is also relevant to those members of the public, including citizen journalists, who are actively involved in sharing information with others, including authorities and CSO's. Whilst an individual may choose to utilise certain privacy restrictive settings on their social networking sites or blogs, that is not to say that the information they do publicly reveal about themselves will not inadvertently reveal important information about their identity.[116] This can be attributed to the challenge of dealing with "weak identifiers", that is "pieces of information that can be used to identify individual users".[117] As illustrated by Palen et al. there are a range of techniques that can be used to remove weak identifiers, however, they argue that within crisis management, it may be more effective to "allow users to have a high degree of control and flexibility with respect to the types of personally identifying information revealed", and thus communication and transparency is required in obtaining consent.[118] As will be seen in the subsequent section, the difficulty of remaining anonymous and safeguarding an individual's anonymity is of particular importance to ensuring a persons' security.

Ensuring anonymity during a crisis is one challenge, a second challenge is ensuring that a person's data remains anonymous when organisations and third parties (e.g., researchers) utilise information shared during a crisis to further understand the crisis at a later date (i.e., for research purposes). This is of particularly importance when terms and conditions from some social networking sites, e.g., Twitter, emphasise the "re-use" of data.[119] For instance, in their study of the use of Twitter by the London Metropolitan Police and Manchester Police following the 2011 summer riots in the UK, Bartlett and Miller took measures to ensure that they upheld ethical principles of ensuring anonymity:

> "…we carefully reviewed all tweets selected for quotation in this report and considered whether the publication of the tweet, and the links, pictures and quotations contained within, might result in any harm, distress, to the originator or other parties involved. For example, if any possibly invasive personal information were revealed in the body of the tweet, this was not used. As a further measure, we removed any user names; and in a small number of cases, 'cloaked' the text so it could not allow for the identification of the originator".[120]

Thus ensuring anonymity should be an important consideration in the ethical re-use of other people's data.

[114] Rive, G., Hare, J., Thomas, J. and Nankivell, K. "Social Media in an Emergency: A Best Practice Guide", Wellington Region CDEM Group: Wellington, 2012. http://www.gw.govt.nz/assets/Emergencies--Hazards/WREMO/Publications/Social-media-in-an-emergency-A-best-practice-guide-2012.pdf [p. 19]

[115] American Red Cross, "Social Media Handbook for Red Cross Field Units", *American Red Cross, Slideshare,* 17 July 2009. http://www.slideshare.net/wharman/social-media-handbook-for-red-cross-field-units, slide 87.

[116] Yates et al., 2009, p. 6.

[117] Palen et al., 2010, p. 9.

[118] Ibid.

[119] Bartlett and Miller, 19 June 2013, p. 5.

[120] Bartlett, J. and Miller, C. "@metpoliceuk how twitter is changing modern policing: the case of the Woolwich aftermath", *DEMOS,* 19 June 2013. [p. 6]

3.1.4 Privacy and surveillance

As discussed in Deliverables 2.1 and 2.2 of the COSMIC project, the use of GPS based services integrated into new media applications including, Facebook, Twitter, Google Maps and so forth, mean that individuals provide others with access to their personal data regarding their location, which may contribute to responders abilities to manage a crisis, particularly in locating individuals.[121,122] To illustrate, following their study of the disruption caused by the ash cloud stemming from the Eyjafjallajokull volcano in 2010, Reuter et al., advocated the use of tagging and geo-tagging of social network based content (e.g., the sharing of photographs and messages on Twitter), to help crisis managers determine the precise location of an incident.[123] However, as identified by Watson and Finn, such practices have the potential to affect an individual's privacy of location[124], therefore requiring clear policies from authorities regarding the secondary use of the data they collect and receive via their interactions with social media.

Data retention for secondary use following a crisis can also be seen to be problematic in terms of threatening a person's privacy when collected and stored for intelligence purposes, thereby being a form of surveillance; data surveillance, otherwise referred to as dataveillance. As identified by Clark, dataveillance involves "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons".[125] The expanse of digital technology and the ever-growing emphasis on the use of big data for analytics means that the collection and examination of personal data for monitoring is becoming more common place and promoted as a tool for investigative purposes, including disaster response activities.[126] Dataveillance greatly impacts Finn et al's "privacy of data and image" which "includes concerns about making sure that individuals' data is not automatically available to other individuals and organisations and that people can "exercise a substantial degree of control over that data and its use".[127]

In relation to crisis management dataveillance raises particular challenges relating to privacy and surveillance and the monitoring of social media. As argued by McCarthy and Yates, "others fear that government agencies involved in disaster response might track, catalogue, or otherwise invade the privacy of public individuals who do decide to help".[128] Similarly, as identified by Lindsay, in the US, concerns relating to the collection, retention and data mining of personal information by the federal government for disaster recovery purposes is seen as a threat as it may be used for investigative purposes; "would the federal government compile

[121] Watson, H, Finn, R., Wadhwa, K., and Yannopoulos, A., "State of the art of communication technology for crisis management", Baseline analysis of communication technologies and their applications, *Deliverable 2.1 of the COSMIC project*, 31 Aug 2013.

[122] Papadimitriou, A., Yannopoulos, A., Kotsiopoulos, I., Watson, H., Baruh, L., "Case studies of communication media and their use in crisis situations", *Deliverable 2.2 of the COSMIC project,* 30 September 2013.

[123] Reuter, C., Marc, A. and Pipek, V., "Social Software as an Infrastructure for Crisis Management - a Case Study About Current Practice and Potential Usage". *Proceedings of the 8th International ISCRAM Conference*, Lisbon, Portugal, 2011.

[124] Finn et al., 2013.

[125] Roger Clarke, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms", *Xamax Consultancy*, Aug 1997. http://www.rogerclarke.com/DV/Intro.html

[126] Almon, G., "The Conversation About Big Data in Crisis/Disaster Response Is Happening Now." *Tech 4 Relief,* 27 June 2013. http://www.tech4relief.com/2013/06/27/the-conversation-about-big-data-in-crisisdisaster-response-is-happening-now/

[127] Finn et al., 2013, p. 8.

[128] Yates and Paquette, 2010, p. 12.

records after a terrorist attack to help investigate certain individuals?"[129] As identified in D2.2 of the COSMIC project, during the Boston marathon attacks in 2013 this could have been problematic, not only as authorities, including the Boston police, had asked for members of the public to submit photographs to them to help with the investigation, but furthermore, as will be seen in the next section, the use of data for surveillance purposes can also lend itself to security issues relating to digital volunteerism and the miss-labelling of individuals for investigation purposes.[130]

Bartlett and Miller have examined the use of social media for intelligence (SOCMINT) purposes in their study of the use of Twitter by the London Metropolitan police during the Woolwich attacks in 2013, where they found both opportunities and challenges for policing with regards to the use of social media. A crucial challenge they identified includes:

> "…there are legal and ethical questions – still open – as to how the police can collect and use social media information in a way that is proportionate, legal and can command public confidence and support. The official collection and use of social media information is a controversial and contested practice, especially for the purposes of intelligence and security".[131]

In Europe this is of particular importance. As examined by the EU project COMPOSITE in their study of police officers attitudes to the use of social media in policing, social media was seen to have a "perceived value" in that it had the potential to be used for a range of services including: notifying disaster-related issues, notifying crime problems, public relations, intelligence, listening/monitoring etc.[132] Thus, adequate consideration is required relating to how to improve the security of the citizen without undermining citizen's privacy and trust.[133] The challenge of new media applications and their impact on surveillance will be further examined in the final version of this deliverable.

3.2 Security

Whilst the use of social media in a crisis has its benefits, there are also a series of security related challenges that must be taken into consideration concerning the emphasis placed on the use of new media applications, including social media in relation to crisis management activities. Accordingly, within this sub-section, partners will explore issues relating to information security, challenges surrounding the reliability of information and the physical security of individuals involved in using social media during a crisis.

3.2.1 Protection of information from loss or theft

The challenge of ensuring and safeguarding information is of the utmost importance to the use of new media applications in crisis management activities. As argued by Dlamini et al. information security is not a new concept, rather the need to secure information is "as old as information itself", for we have long been concerned with securing the transmittance, stored

[129] Lindsay, 2011, p. 7.

[130] Papadimitriou et al., 2013.

[131] Bartlett and Miller, 19 June 2013, p. 17.

[132] Bayerl, S. P., "Social Media Study in European Police Forces: First Results on Usage and Acceptance", *Preliminary report from the COMPOSITE project,* 29 September 2012. [p. 12]

[133] Bartlett, J., Miller, C., Crump, J., and Middleton, L. "Policing in an information age", *DEMOS, CASM policy paper,* March 2013.

and processed.[134] Dlamini et al. chart the historical background of information security citing key moments in history such as the need for encryption to secure the telegraph in the 1840's, as well as the risk posed by the remote use of data in the 1960's. As technology has progressed so too has the threats and risk we are faced with to ensure the security of information. The 21st Century is typified by a "strong dependence on IT infrastructure" which has brought with it opportunities for the "hacking community", both in terms of providing a source of "fun" and a challenge, as well as providing a means for financial gain.[135] Consequently we are faced with information related threats including (but not limited to), identity theft, social engineering, phishing, sabotage, malware attacks etc.[136, 137, 138] For instance, following the Boston marathon attacks in April 2013, cyber gangs utilised the attacks, along with a devastating explosion of a Texas fertiliser plant to conduct a phishing scam. The scam involved encouraging users to view a YouTube video of the events, which then triggered an infection in the user's computer.[139]

When considering information security in relation to crisis management activities, as identified by Yates et al. there is a danger that following some crises, the mining of data by some could be used for identity theft as well as other malicious activities targeted at vulnerable groups. As noted by Yates et al., even when personal identity information may be masked, as discussed in the previous sub-section, there is still the threat that the collection and analysis of weak identifiers could lead to uncovering a person's true identity.[140] Such a threat may be particularly dangerous when considering the use of new media applications such as Facebook and Twitter in political crises.[141] For instance the sharing of perspectives by citizen journalists, as well as any physical evidence (e.g., photographs, video footage etc.) that they may share, may put both themselves and others at risk in highly volatile political situations. This may be particularly troublesome if there is the potential danger of any identifiable information being shared or subsequently collected by others for intelligence purposes.

In order to take measures to help ensure the safety of information, and the anonymity of a person's personal data, as identified by the ICRC, organisations should take steps to ensure that they "analyse the different potential risks linked to the collection, sharing or public display of the information and adapt the way they collect, manage and publicly release the information accordingly".[142] Thus awareness by organisations involved in sharing information and promoting the sharing of information should acknowledge and outline the risks associated with it via new media applications, which in turn places emphasis on the need for digital literacy and a wider understanding of the various online threats. Furthermore, the need for greater understanding regarding threats to information security means greater responsibility

[134] Dlamini, M.T., J.H.P. Eloff, and M.M. Eloff, "Information Security: The Moving Target." *Computers & Security*, Vol. 28, No. 3–4, May 2009, pp. 189–198.

[135] Dlamini et al., 2009, p. 191.

[136] Dlamini et al., 2009, p. 191.

[137] Geers, K. *Strategic cyber security,* NATO Cooperative Cyber Defence Centre of Excellence, CCD COE Publication, Estonia, June 2011.

[138] Martin, N., and Rice, J. "Cybercrime: Understanding and addressing the concerns of stakeholders", *Computers & security*, Vol. 30, 2011, pp. 803-814.

[139] Acohido, B. "Phishing campaign leverages news of bombings, explosion", *The Last Watchdog on Internet Security [Blog],* 19 April 2013. http://lastwatchdog.com/phishing-campaign-leverages-news-bombings-explosion/

[140] Yates, David, and Scott Paquette, "Emergency Knowledge Management and Social Media Technologies: A Case Study of the 2010 Haitian Earthquake", *International Journal of Information Management*, Vol. 31, No. 1, February 2011, pp. 6–13. [p. 12]

[141141] Palen et al., 2010, p. 8.

[142] ICRC, 2013, p. 86.

for data security on part of the various different types of stakeholders involved in crisis management activities.

As part of the EU Directive 95/46/EC on data protection, website operatives and organisational rules require attention to data security. As identified by Jones and Tahri, whilst the Directive "does not specify what particular measures must be in place, other than that they should ensure a level of security appropriate to the nature of the data to be protected and the risks associated with unauthorised or unlawful processing and accidental loss, destruction or damage".[143] Ensuring the security of information also involves the integration of data security practices such as "handling and treatment" of personal and confidential information, e.g., through limiting the collection of data with personal content, install electronic security codes of practice and monitoring physical and electronic access to sensitive information.[144] Once again, in light of the threat to individuals involved in political crises that are turning to social media as an outlet for disseminating their own views and news, there is a need to ensure the physical security of information, particularly sensitive information. As outlined by the ICRC, "Security safeguards appropriate to the sensitivity of the information must be in place prior to any collection of information, to ensure protection from loss or theft, unauthorized access, disclosure, copying, use or modification, in any format in which it is kept".[145] At the same time it is necessary for individuals themselves to consider the potential threat to their security in sharing personal information. Consequently, nation states should, as identified by Martin and Rice, consider the need for education and awareness raising activities to help protect individuals from those threats they may have from sharing information online.[146]

3.2.2 Reliability of information

As will be extensively discussed in Deliverable 2.3 of the COSMIC project; "Report on the adverse use and reliability of new media"[147], the reliability of information is indeed an important challenge to security that should be taken into consideration by those engaging with new media applications as part of their crisis management activities.

As identified by Lindsay, information that is "false, inaccurate or outdated could complicate the situational awareness of an incident and consequently hinder or slow response efforts. Inaccurate information could also jeopardize the safety of first responders and the community". [148] To illustrate, following wildfires in California in August 2013, authorities asked residents not to turn to social media for fire-related updates as the number of digital rumours circulating caused some individuals to feel a heightened sense of anxiety and fear (e.g., the Groveland firehouse had burned down; authorities were cutting power lines to force people to evacuate; police had arrested an arsonist who started it etc.).[149] As Watson and Wadhwa argue, there is therefore a need for authorities to be particularly conscious of the abilities of social media to function as a rumour mill, however, there are tactics such as the adoption of verification practices and active monitoring and debunking of rumours that

[143] Jones and Tahri, 2011, p. 633.

[144] Martin and Rice, 2011, p. 807.

[145] ICRC, 2013, p. 91.

[146] Martin and Rice, 2011.

[147] Due: November 2013.

[148] Lindsay, Bruce R., *Social Media and Disasters: Current Uses, Future Options, and Policy Considerations*, CRS Report for Congress, Congressional Research Service, 2011. http://www.fas.org/sgp/crs/homesec/R41987.pdf [p. 7]

[149] Carroll, R., "California Officials Ask Residents to Avoid Social Media for Rim Fire Updates." *The Guardian*, 27 August 2013. http://www.theguardian.com/world/2013/aug/27/rim-fire-california-social-media-avoid

authorities and response organisations can employ to help quell rumours and reduce public concerns.[150]

An example of industry responding to opportunities for their products in crisis management activities includes the newly launched Twitters alert service, where officials and NGO's can sign up to Twitter's Alert Service to send official alerts using a specialised Tweet composer to create a Tweet and tag it as a critical alert to be pushed to their subscribers via a notification or SMS message. Such a service may help to divert users' attention to more "official" sources of information on social media.[151]

In addition to the spreading of false rumours, there may also be the danger of some individuals utilising other people's social media use (including response organisations) for malicious purpose, and thus organisations should, as identified by Lindsay, "develop measures to mitigate those possibilities".[152] As outline by Palen et al., under cyber terrorism conditions, malicious users may deliberately contribute false or misleading information which could subsequently disrupt efforts of "self-policing and accuracy attainment".[153] Accordingly, as identified by the ICRC, organisations utilising social media for managing a crisis should try to be "explicit as to the level of reliability and accuracy of information they use or share".[154] Similarly, as argued by Humanity Road, a virtual volunteer organisation working within the domain of disaster response to inform the public on how to survive after a crisis, the use of social media, such as Twitter by volunteers should be conducted along a "do no harm" principle, for instance: "It is safer to share no news than to share inaccurate news. Rumours put lives at risk".[155]

3.2.3 The security of the citizen

As indicated to in this chapter, challenges relating to privacy and security can indeed have an impact on citizens, whether it be from misuse, loss or theft of their personal data, or by malicious attacks. However, it is important to consider other security related impacts on the security of the citizen. In particular, this sub-section will briefly consider those issues relating to vigilante justice and the physical safety of individuals operating in volatile areas.

As examined by Finn in Deliverable 2.2 of the COSMIC project, following the 2013 Boston marathon attacks, there was extensive evidence of the use of the social networking site, Reddit, by citizens to gather pictorial evidence (as also requested by the Boston Police) from the scene of the Boston attacks, where users were invited to share their images. This led to some individuals seeking to take efforts into their own hands to identify those responsible, leading to the wrongful identification of innocent victims. Thus, crowdsourcing behaviour in the face of a crisis, if un-regulated can lead to the risk of innocent individuals being inappropriately labelled and targeted.

[150] Watson, H. and Wadhwa, K. "The evolution of citizen journalism in crises: From crisis reporting to crisis management" in Allan, S., and Thorsen, E. *Citizen Journalism: Global Perspectives, Volume Two*. Peter Lang. [Forthcoming]

[151] Twitter, "A step-by-step guide to Twitter Alerts", *Twitter Alerts,* 2013. https://about.twitter.com/alerts/how-it-works

[152] Lindsay, 2011, p. 7.

[153] Palen et al., 2010, p. 8.

[154] ICRC, 2013, p. 89.

[155] Starbird, K., and Palen, L., "Working & Sustaining the Virtual "Disaster Desk", Computer Supported Cooperative Work and Social Computing (CSCW), 23-27 February 23 2013, San Antonio, Texas, USA. [p. 3].

Similarly, as identified by Rizza et al., vigilante justice was also present following the ice hockey Stanley Cup final series between the Vancouver Canucks and the Boston Bruins which took place in Vancouver in June 2011 leading to riots. The riots led to individuals taking it upon themselves to publicise the riots via social media, and to share information and data (upon request) with authorities of who they believed rioters to be. Furthermore, they then engaged in "do it yourself justice" by publicly damning those responsible via social networking sites, which has been labelled a form of "bad ethics" by Henry (2011).[156] Thus, law enforcement agencies should consider the impact of requesting information and content via social media for any potential use and should subsequently take measures to ensure that they publicise how *they* will utilise the information. As identified by Rizza et al., perhaps there is a need for "authorities to establish clear rules regarding citizen cooperation in a crisis situation".[157] Similarly, there is a need for greater education on part of the public, to help emphasise the need for restraint in participating in targeted digital volunteerism.

Lastly, it is necessary for organisations and members of the public to consider the safety of those individuals participating in the collection of information to be shared via social media to help understand and manage a crisis. As noted by Watson, there is the risk that individuals could place themselves in danger to record information, and could subsequently need further help from authorities. Similarly, there is the ethical dilemma involved in participating in citizen journalism. As argued by Bakker and Paterson, following the 2005 London attacks, the capturing of graphic images of the attacks, particularly those affected, could be seen as a form of citizen paparazzi, where citizens' may be more concerned with capturing a newsworthy photo, rather than staying out of the way, or in extreme cases stepping into help. Whilst these may seem like extreme cases, encouraging graphic evidence from those at the scene of a crisis, particularly by the media in their efforts to publicise an event, could place individuals in danger. Thus, it is necessary to consider the ethical dimension of citizen involvement by different stakeholders that may have an interest in participating in utilising social media to gather material from those at the scene of a crisis.[158]

3.3 CONCLUSION

This chapter has sought to identify and discuss some of the privacy and security related challenges that those utilising new media applications to contribute to crisis management should consider and take measures to respond to. Building on from Chapter 2 of this report, partners identified EU policies on data protection that stakeholders should be aware of, understand and accordingly, implement measures and policies to ensure that the sufficient steps are taken to meet data protection regulations for the sharing, collection and re-use of data for secondary purposes. Partners also discussed the various privacy related issues for stakeholders to consider: including transparency, legitimate purpose, data protection, anonymity and the impact of data collection on surveillance. Finally, partners discussed the various challenges surrounding the protection of information as well as the potential impact of the use of new media technologies on citizens' safety.

[156] Rizza, C., Pereira, C., and Curvelo, P. ""Do-it-yourself justice": considerations of social media use in a crisis situation: the case of the 2011 Vancouver riots", *Proceedings of the 10th International ISCRAM Conference,* Baden-Baden, Germany, May 2013.

[157] Rizza et al., 2013, p. 6.

[158] Watson, H., "Dependent Citizen Journalism and the Publicity of Terror", *Terrorism and Political Violence*, Vol. 24, No. 3, 2013, pp. 465-482.

Overall, this preliminary discussion of the various privacy and security related challenges to the use of social media in crisis management activities has, where possible, illustrated the need for greater emphasis to be placed on organisations, and in some cases, members of the public, to ensure that they take measures to sufficiently protect those with whom they are interacting, for they may be affected by the actions of others.

This analysis will be further developed within the COSMIC project as part of partners' on-going work into the various social opportunities and challenges regarding the use of new media applications in crisis management.

4 OVERALL CONCLUSIONS

The present document focused on policies, standards and privacy and security issues in the context of mass utilisation of emerging technologies and information gathering/sharing via social media.

The first part (chapter 2) examined existing policies, standards and opportunities relating to social media and crises. On the policy front, applicable measures taken at EU level cover the areas of privacy, data protection and telecommunications. Current EU legislation concerns the Directive on data protection (1992) and the "Telecommunications Package" and its updates. Policy directions contained in the Digital Agenda point to the need for regulatory intervention on emerging issues such as the openness of the Internet and the freedom of citizens to access and run applications and content.

The partners highlighted the relevance of the reform of the current Data Protection Directive, proposed by the European Commission, and, in particular, its provision for added protection of online data via the "right to oblivion" (Article 17). On the telecommunications side, the implications of the, as yet unsettled, issue of the lack of an EU-wide imposed minimum bandwidth obligation on a Universal Provider were noted as a pending policy issue potentially affecting social network based communication, especially during a crisis.

The question of standardisation in social media was found to affect aspects such as compatibility, interoperability, safety and quality both from the point of view of the industry as well as the consumers. The partners examined standardisation challenges such as the underlying telecommunications technologies, the presentation layer of social media, the data involved and the means of interacting with social media services. For the semantics-rich social media data, representation mechanisms such as Linked Data were identified and commented upon, along with various emerging attempts for describing semantic models. In addition, examination of the developing and varied landscape of tools for interacting with social media services revealed the complex interplay between market leaders and their competitors and correspondingly between proprietary and open standards.

The second part (chapter 3) has sought to identify and discuss some of the privacy and security related challenges that those utilising new media applications to contribute to crisis management should consider and take measures to respond to. Building on from chapter 2, partners identified EU policies on data protection that stakeholders should be aware of, understand and accordingly, implement measures and policies to ensure that the sufficient steps are taken to meet data protection regulations for the sharing, collection and re-use of data for secondary purposes. Partners also discussed the various privacy related issues for stakeholders to consider: including transparency, legitimate purpose, data protection, anonymity and the impact of data collection on surveillance. Finally, partners discussed the various challenges surrounding the protection of information as well as the potential impact of the use of new media technologies on citizens' safety.

Overall, this preliminary discussion of the various privacy and security related challenges to the use of social media in crisis management activities has, where possible, illustrated the need for greater emphasis to be placed on organisations, and in some cases, members of the public, to ensure that they take measures to sufficiently protect those with whom they are interacting, for they may be affected by the actions of others.

This analysis will be further developed within the COSMIC project as part of partners' on-going work into the various social opportunities and challenges regarding the use of new media applications in crisis management.