SECURE DYNAMIC CLOUD FOR
INFORMATION, COMMUNICATION AND RESOURCE INTEROPERABILITY
BASED ON PAN-EUROPEAN DISASTER INVENTORY

Deliverable 2.2

ELSI Guidelines for collaborative design and database of representative emergency and disaster events in Europe

Final Version

Katrina Petersen

Centre for Mobilities Research, Department of Sociology, Lancaster University

March 2015

Work Package 2

Project Coordinator

Prof. Dr.-Ing. Rainer Koch (University of Paderborn)

7th Framework Programme

for Research and Technological Development

COOPERATION

SEC-2012.5.1-1 Analysis and identification of security systems
and data set used by first responders and police authorities

Distribution level		Public		
Due date		13/03/2015		
Sent to coordinator		13/03/2015		
No. of document		D2.2		
Name		*ELSI Guidelines for collaborative design and database of representative emergency and disaster events in Europe*		
Type		*Report*		
Status & Version		*Final Version 1.0*		
No. of pages		*83*		
Work package		*2*		
Responsible		*ULANC*		
Keywords		*ELSI, collaborative design, common information space*		
History	Version	Date	Author	Comment
	V0.1	14/12/2014	ULANC	Initial draft and outline
	V0.2	28/1/2015	ULANC	Revised draft and outline
	V0.21	2/2/2015	UPB	Contributions/Comments
	V0.22	5/2/2015	KEMEA	Contributions/Comments
	V0.23	11/2/2015	TUDO	Contributions/Comments
	V0.3	11/2/2015	ULANC	Revised Draft for Internal Review
	V0.4	12/3/2015	ULANC	Revisions post QA Review/Monitoring
	V1.0	13/03/2015	UPB	Final Version and submission

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n°607832.

Authors

	University of Paderborn C.I.K.	Steffen Schneider Email: st.schneider@cik.upb.de
	Mobilities.Lab Centre for Mobilities Research Department of Sociology Lancaster University LA1 4YD UK	Monika Buscher Email: m.buscher@lancaster.ac.uk Katrina Petersen Email: k.petersen@lancaster.ac.uk Sarah Becklake Email: s.becklake@lancaster.ac.uk Vanessa Thomas Email: v.thomas1@lancaster.ac.uk Catherine Easton Email: c.easton@lancaster.ac.uk Rachel Oliphant Email: r.oliphant@lancaster.ac.uk Xaroula Kerasidou Email: x.kerasidou@lancaster.ac.uk
	British APCO	Paul Hirst Email: paul.hirst@bapco.org.uk
	Center for Security Studies (KEMEA) P.Kanellopoulou 4 1101 77 Athens Greece	Ioannis Daniilidis Email: i.daniilidis@kemea-research.gr Dimitris Kavallieros Email: d.kavallieros@kemea-research.gr
	TU Dortmund CNI	Maike Kuhnert Email: maike.kuhnert@tu-dortmund.de
	T6 Ecosystems	Katja Firus Email: k.firus@t-6.it

Reviewers

AIRBUS DEFENCE & SPACE	Airbus Defense and Space	Daniel Zerbib Email: daniel.zerbib@airbus.com Olivier Paterour Email: Olivier.Paterour@airbus.com
UNIVERSITÄT PADERBORN Die Universität der Informationsgesellschaft c.i.k.	University of Paderborn C.I.K.	Steffen Schneider Email: st.schneider@cik.upb.de

Executive summary

This deliverable develops an analysis of ethical, legal and social issues (ELSI) arising in the context of designing a secure dynamic cloud and common information space concept for multi-agency crisis management – the central objective of the SecInCoRe project[1]. This is based on a Pan-European inventory or database of representative emergency and disaster events in Europe, which will also gather information about data sets, command systems and information management processes, information systems and business models. The aim of this report is to work towards ethically, legally and socially sensitive collaborative design methods and products.

This report begins to formulate ELSI Guidelines to this end. These are derived from a mixed methods research process that combines literature review with interviews with experts and a co-design approach that draws the knowledge and expertise of a diverse group of stakeholders and publics into the innovation process.

The analysis and guidelines contribute to all four key objectives of the project in a number of ways (see Table 1). First, it sensitises designers, users and indirectly affected publics to ethical, legal and social dimensions of categorisation and inventory-making, highlighting opportunities and challenges. Second, it draws attention to opportunities and challenges in actually supporting real world collaborative work practice, information politics, organizational culture, whilst detailing threats of technology dependence, frictions around data protection regulations, digital divides, social sorting. Third, the aim is to sensitise designers to the socio-technical nature of innovation, highlighting opportunities and challenges arising from such a more integrated perspectives. And forth, this serves to define the object of evaluation in a more complex but also more adequate and ambitious way as a socio-technical configuration of technologies, practices, policy, regulatory frameworks. This serves to establish a human-centered, value sensitive collaborative design and responsible research and innovation methodology and it can help structure and enrich formative and summative evaluation.

After the explanation of the general purpose and structure of the document in chatper 1, the deliverable is structured into six main parts, each chapter building on the previous ones.

Chapter 2 introduced the problem of ELSI and why they are important for SecInCoRe. It explores the gaps in already established ELSI guidelines. Pairing our role as co-stewards in the design process with the notion the ELSI emerge in design, not a priori, the section sets the stage for the issues to follow.

Chapter 3 explores previous literature on issues related to looking for technological solutions to cross-border interoperability in disaster response. First it establishes the present conversations in disaster ethics and their relative inattention to IT use. It then examines Science and Technology studies theories of technology and users to argue that the two cannot be separated, nor can programmable rules address ELSI as they arise because ELSI are defined not by what ‘privacy’ or ‘security’ mean but by who decides on the meaning, to what effect and how. In other words, privacy and security

[1] http://www.secincore.eu

cannot be designed, but are practices that can be designed for. It then explores the ELSI that become evident in the use of standards, classifications, and archives, key issues when managing an inventory, to find that these systems produce meanings and histories rather than describe them, and in doing so have the potential to produce ideals and norms that should not necessarily be applied from one situation to another. The section finishes by examining how these issues can be engaged with when looking forward instead of backwards, and how they argue for and inform human-centred design.

Chapter 4 similarly looks to previous literature, but focused on cases of data-gathering and exchange: smart cities, weather, social media, and border security and surveillance. It does so to, again, pull out the ELSI dealt with in each of these cases. In smart cities we find that more technology or data does not necessarily make one smarter, and even what smarter means is contested. In data-sharing around weather, scientists are often faced with extreme questions of responsibility: are they stewards to the scientific practices or the national politics? Are they dealing with public goods or market logics? Looking at social media publics it becomes clear that publics, plural, need to be accommodated in ways that balance formal response structure with emergent cultural classifications. Examining border surveillance makes clear that security is complicated and often contradictory. We must ask what is being protected and prioritized: security to move across borders or security of people within a border?

Chapter 5 Assembles the lessons from Chapter 3 and 4 with the trends found in the case studies in D2.1 as well as the results and observations from the Co-Design Workshop in December 2014 to establish a set of ELSI that carry throughout the design process, from conception to use. These issues include: Access and Equality, Pre-emptive Risk Assessments, Local and International Legal and Regulatory Changes, Delimiting Liabilities, Balancing Data Sharing and Privacy, Sharing and Trust, Privatization of Public Goods, Management and Democratic Participation, Balancing Security and Surveillance, Aligning Local Meaning Making, Designing for Responsibility, Simplicity, Adaptability, Scalability, Inclusiveness, Translation and Diversity, Transparency, Making Useful Technology

Chapter 6 turns these ELSI into guidelines for human-centred research design. These guidelines argue that this type of research needs to actively include stakeholders in ways that encourage the envisioning of new solutions and ways of defining problems that otherwise would have gone unimagined. Among the guidelines are a aim for hands-on understandings that covers a wide range of stakeholders, that always explores the interplay between the social, technological, and organizational in various contexts. It also needs to encourage culture clashes as well as moments of tension and negotiation to encourage mutual learning and the highlighting of tacit practices.

Chapter 7 turns these ELSI into a preliminary set of guidelines for SecInCoRe's design process, specifically exploring the issues around the 3 main objectives: the Pan-European Inventory, the Common Information Space, and the Network Infrastructure. In doing so, it establishes specific ELSI that will need to be addressed throughout design (rather once design is complete and the system is in use) and for assembles these issues into specific guidelines for which potential solutions are provided.

Table of contents

1 Introduction

1.1 Purpose of this document

The purpose of this report is to establish initial guidelines for design and organizational innovation that is sensitive to ethical, legal, and social issues (ELSI) regarding data sharing during large-scale disaster response (WP2). To do so, it draws on related projects in the disaster response domain and related projects in other domains, such as smart city endeavours, earth observation systems, social media publics, and cross-border security management in order to learn from issues already encountered in similar socio-technical systems (T2.1). From there, it establishes a human-centred, value sensitive collaborative design and responsible research and innovation methodology that focuses on technologies in practice and technological expectations (T2.3). The aim is not just to design for users and their already demonstrated user needs, but to also envision new ways of working and new approaches to technology design and use in collaboration with a broad range of users. The results are intended to influence the design of the Inventory, CIS, and network infrastructure for the secure dynamic cloud for information communication and resource interoperability (WP3 and WP4). This also sensitises the team to how everyday practice might change and new organizational possibilities may arise from enhanced interoperability in a way that can be validated throughout the design process (WP5 and T2.4). The final aim is to suggest ELSI guidelines for each component of the SecInCoRe project, guidelines that structure both the design concepts but also additions to the inventory of exemplary disaster events.

1.2 Validity of this document

This document is derived from a mixed methods research process, including a co-design workshop with response experts from a range of European countries, a literature review of previous research, and research done in other interoperability contexts, such as smart city design efforts, social media publics and cross border security. While the empirical base is not extensive, it builds upon existing knowledge in the consortium and speaks directly to this project by incorporating a variety of background and experience levels, providing a solid background that covers a range of EU and other countries, previously existing ELSI guidelines and recommendations from EU projects in general, and data sharing practices to the conceptualization required for this project. The data used in this deliverable should be measured in terms of variety and scope rather than sheer numbers.

1.3 Relation to other documents

This document is based on tasks T2.1 (Overview of disaster events, crisis management models and stakeholders) and T2.3 (Formulation of user goals and ethical, legal and social issues) and has relationships with many other documents created within the SecInCoRe project, including, most importantly:

Inputs:

[1] Grant Agreement (no. 607832) and Annex 1. - Description of Work

[2] Consortium Agreement

[3] D1.2 Research Ethics (first version): Research Ethics Protocols, relevant authorisations and informed consent

[3] D2.1 (WP-2) – 'Overview of disaster events, crisis management models and stakeholders' [in the form of T2.1; T2.2 input to T2.3]

[4] D3.1 (WP-3) – 'Setup of inventory framework and specification of research requirements' [in the form of T3.1/T3.2 as related to T2.1/T2.3; T3.4 as related to T2.1]

Outputs:

[5] D2.3 (WP-2) – 'Report on Performance, Goals and Needs and First Draft of New Crisis Management Models and Ethical, Legal and Social Issues' [in the form of T2.3; T2.3 as input to T2.4]

[6] D2.4 (WP-2) – 'Domain Analysis: Baseline and Emergent Future Practices' [in the form of T2.1; T2.1 as input to T2.2]

[7] D2.7 (WP-2) – 'ELSI in Crisis Management through the Secure Dynamic Cloud' [in the form of T2.3 input to T2.4]

[8] D3.2 (WP-3) (being written in parallel) – 'First Publication of Inventory Results' [in the form of T2.1/T2.3 as related to T3.1/T3.2; and T2.1 as related to T3.4]

[9] D3.3 (WP-3) – 'Second Publication of Inventory Results, including Ethnography and Holistic Process Models and Statements on Future Evolutions' [in the form of T2.1/T2.3 input to T3.1/T3.2; T2.1 as input to T3.4]

[10] D3.4 (WP-3) - Final Publication of Inventory Results' [in the form of T2.1/T2.3 input to T3.1]

[11] D4.1 (WP-4) – 'Requirements Report' [in the form T2.1/T2.3 input to T4.2]

[12] D4.3 (WP-4) – 'Network Enabled Communication System Concept and Common' [in the form of T2.1/T2.3 input to T4.1]

[13] D4.4 (WP-4) – 'Report on Interoperability Aspects' [in the form of T2.1/T2.3 input to T4.1]

[14] D5.2 (WP-5) – 'Early Setup of Evaluation Model for Internal Use Cases' [in the form of T2.1/T2.3 input to T5.2]

[15] D5.3 (WP-5) – 'Validation Strategy and First Functional Evaluation Model of Communication System Concept' [in the form of T2.1/T2.3 input to T5.2]

1.4 Contribution of this document

The work documented here contributes to all four key objectives of the project in different ways (Table 1).

Objective	Contribution of work documented in D2.2
• **Curation of a pan-European inventory** of past critical events and disasters and their consequences.	Sensitising designers, users and indirectly affected publics to ethical, legal and social dimensions of categorisation and inventory-making, highlighting opportunities and challenges.
• **Design of a secure, dynamic cloud based knowledge base and communication system concept** including the ability to use emergency information by means of a trans-European communication infrastructure.	Sensitising designers, users, indirectly affected publics to opportunities and challenges in collaborative work practice, information politics, organizational culture, technology dependence, data protection, digital divides, social sorting.
• **Conceptual integration of available ICT technology** into patterns of infrastructure found in first responder organisations.	Sensitising designers to the socio-technical nature of innovation, highlighting opportunities and challenges.
• **Evaluation and validation of all results** in representative fields of application.	Defining the object of evaluation as a socio-technical configuration of technologies, practices, policy, regulatory frameworks. Establishing a human-centred, value sensitive collaborative design and responsible research and innovation methodology. Structuring and enriching formative and summative evaluation.

Table 1 Contribution to Objectives

Probably the most significant contribution is the way in which the analysis can sensitise the project team and potential users and exploitation actors to the complex opportunities and challenges tied into the innovation pursued by SecInCoRe. The analysis and the ELSI guidelines are meant to scaffold creative engagement with these opportunities and challenges in the SecInCoRe project, opening up conversations and linking the efforts of WP2 into the activities of all other WPs (Figure 1).

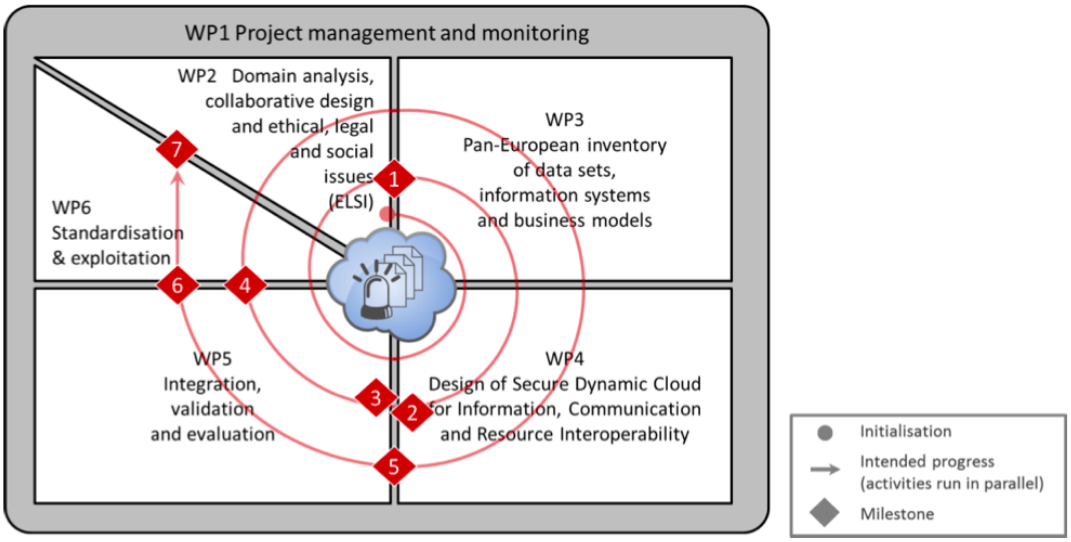

Figure 1 Integration of D2.2 Contribution through SecInCoRe WPs

Rich descriptions of complexities detailed in WP2, maps of data sets, command and information management systems and business models in WP3 will be addressed through formulation of requirements and architectural or non-functional qualities in WP4 and inform integration, validation and evaluation in WP5, as well as standardisation and exploitation in WP6. This interdisciplinary collaboration is based on an open research ethics protocol that details our approach to working with human participants in research, outlined in D1.2 (Research Ethics) and the research ethics section on the project website. Based on studies of real world practice and in-depth engagement with stakeholder expertise such collaboration can drive responsible, circumspect research, innovation and exploitation that can allow European societies to balance security and freedom more effectively in a 21st Century that has been labelled the 'Century of disasters' (eScience, 2012).

1.5 Target audience

The document provides an overview of ethical, legal and social issues arising in relation to the curation of a pan-European inventory of past disaster events and the design of a dynamic cloud and common information space concept. The analysis and guidelines are meant to underpin collaborative research and innovation within the SecInCoRe team. We make this public to engage the wider scientific and practitioner communities in the debate. The document is mainly aimed at researchers in different disciplines, interested practitioners and policy makers.

1.6 Glossary

Collaboration in an interdisciplinary team requires some 'translation' between domains and academic disciplines. In this deliverable, we define ethical, legal and other terms as they are introduced, and provide links to the literature where they are discussed in more depth. The short glossary below supplements such in-text definitions.

Abbreviation	Expression	Explanation
	Actionable Information	Information presented in such a way that decisions can be made from it.
	Boundary Object	Objects of common concern that may have different meanings for each group engaging with it but that are recognizable as common.
	Collaborative Design	A form of participatory design in which users and designers are brought together to share experience and prototypes in order to imagine emergent futures and foresee design challenges, opportunities, and ELSI.
CEIS		Cloud Emergency Information Space
CIS		Common Information Space
	Crowdsourced	Data gathered using the general public , typically without any specific expertise, that assumes sheer numbers will correct for errors.
	Digital divide	Inequality between groups, in terms of access to, use of, or knowledge of information and communication technologies (ICT) and by extension exclusion from participation in large areas of contemporary society.
	Disclosive Ethics	An approach in the ethics of technology that brings the usually silent and opaque operation of digital technologies to the surface to open it up to critical scrutiny.
	Disruptive Innovation	Innovation that is done is a way to specifically interfere with normative practices such that values, assumptions, and expectations become visible so that new needs can be identified and markets

Abbreviation	Expression	Explanation
		created.
	Distributed Justice	Socially just allocation of resources.
ELSI		Ethical, Legal, and Social Issues
	Emergent Future Practices	Foresight into new ways of doing things that would otherwise go unseen or done without the introduction of a new technology, but are seen neither in the technology nor previous ways of doing things alone.
	Emergent Interoperability	Possibilities for interoperability that develop through present interactions.
IT		Information Technology
	Local Resilience Forum	Multi-agency partnerships made up of representatives from local public services that aim to plan and prepare for localised incidents and catastrophic emergencies.
	Memorandum of Agreement	Document drafted between two agencies that agree upon rules of interactions.
	Mission Creep	Moving a project or mission beyond its original goal or context.
NEC		Network Enabled Communication
NGO		Non-Governmental Organisation
	Normalisation	The adoption of cultural values in social behaviour to the point where they go unquestioned and unnoticed.
	Ontology	The naming of types and their interrelationships with an understanding of how these came to take specific shapes.
	Publics	There is not a single ‘public’, but many

Abbreviation	Expression	Explanation
		different 'publics' depending on location, reason for gathering, purpose of interactions. For example, during a disaster, there is, among others, the affect public, the observing public, the public that offers humanitarian aid, and the public that is unaware.
	Situated Action	First introduced by Suchman (2007), this is the idea that action is inseparable from the context of acting, and these together are part of sense-making.
QoS		Quality of Service
	Situational Awareness	A general picture of a scene that provides an overall scope of the situation being presented.
	Smart City	A city space that uses networked technology in order to gather data about infrastructure, movement of people, etc, in an attempt to be more efficient and better serve its public.
	State of Exception	The notion of normal rules of The State do not apply in disaster situations.
	Stewardship	Long-term maintenance of data that safeguards diversity and authenticity as the data is held for future generations and managed based on their interests, not ours.
	Taxonomy	The science of defining and naming groups on the basis of shared characteristics.
TETRA		Terrestrial Trunked Radio
	Tort Law	Laws that address civil wrong doings, including negligence, defamation, and

Abbreviation	Expression	Explanation
		liability.
	Transparency	In Ethics, transparency means to have the inner workings of a process visible so that anyone using it can understand the steps involved and the implications of those steps. In the realm of information and communication technology, transparency means a system can be used without question or need to think about the processes within.

1.7 List of figures

1.8 List of tables

2 ELSI, Users, Data sharing, and Socio-technical Futures

This deliverable establishes SecInCoRe's initial guidelines for addressing ethical, legal, and social issues (ELSI) that might arise throughout the SecInCoRe design process. The methodological dimension of this has been addressed in detail in D1.2 (Research Ethics) and the research ethics section on the project website. Here, we will elaborate this, but predominantly focus on the IT or socio-technical ethics of developing new concepts, technologies and practices for information, communication and resource interoperability in multi-agency crisis management. While ethical guidelines already exist in many location, including for EU projects themselves (see for example Dratwa, 2014; European Commission, 2013; Pauwels, 2007; Rogerson, 2009; von Schomberg, 2007), they are most commonly focused on issues of data protection, privacy, informed consent, dual use, and work in developing counties, and research on humans or animals. While these issues are crucial to any research project, they leave unaddressed many aspects of ethics in information technology design as well as the non-normative issues often being dealt with in situations of disaster and crisis.

To accommodate for these issues, though, is not as simple as asking the question "how do we make sure the users behave ethically with the system and the data?", because we also have to determine what ELSI issues are at play. A starting place is offered by von Schomberg (2007), with arguments about the need for new collective ethics in light of complex socio-technical practices. But these ideas are presented generically for science and policy, not specifically for disasters or information sharing. Dratwa (2014) explores issues of IT, but primarily in terms of automation, incentives, privacy, human rights, and surveillance. Dratwa (2014) does, however, quite importantly acknowledge that ethics is part of the design process not just something exhibited by the completed design. Each of these frameworks sets part of the stage for SecInCoRe, but none offer a full enough picture to adopt alone.

This deliverable offers the first step to exploring what ELSI means for SecInCoRe. It does so by examining ELSI that have arisen in: 1) previous literature on emergency ethics as well as on ethics surrounding IT use (chapter 3); and 2) related situations, such as other projects for cross-border data exchange or other systems that encourage a widening of interacting stakeholders (chapter 4). Once an initial list of ELSI has been established (Chapter 5), it becomes possible to develop methods to elicit these throughout the design process (Chapter 6) in order for SecInCoRe's treatment of ELSI to evolve as needed and to develop guidelines for ELSI (Chapter 7) that the design process needs to accommodate. As new ethical issues emerge only in use and in relation to (changing) regulatory frameworks, there can be no claim to completeness at this stage.

2.1 Why ELSI when considering data sharing and socio-technical futures?

Ethical, Legal, and Social issues (ELSI) stand at the centre of 7th framework research as a core concern, and this is strengthened further in recent guidance for research (European Commission, 2013, 2014). The aim is to promote responsible scientific and technological progress, focusing on autonomy, beneficience, and justice (Zilgalvis, 2009). All activities funded by the EU must consider ethical and legal issues as integral to the research process and to the production of research excellence

(http://ec.europa.eu/programmes/horizon2020/en/h2020-section/ethics). This is partly a legal requirement based in Decision 1982/2006/EC of the European Parliament and of the Council (Recital 30 and Article 6), requiring all activities comply with these three fundamental ethical principles (http://ec.europa.eu/research/health/policy-issues-ethics_en.html#). This also requires foresight of the ELSI issues likely to emerge from the research and embedding of new technologies (Zilgalvis, 2009). As part of the ethical mandate, research concerning complex socio-technical systems should produce an ethical framework that addresses both the unintentional consequences of socio-technological systems design and collective decisions.

In doing so, the EU is making a clear move towards treating ethics not as an individual responsibility or one that falls only to specific social roles but to one that is a collective co-responsibility. This means that SecInCoRe cannot assume that a specific type of user or use will dictate and manage the ELSI to be faced. This is because roles in society are not easily classified, individuals take on more than one role at a time, and roles are becoming so institutionalized that it is hard to determine what is the responsibility of the individual or the larger institution (von Schomberg, 2007). Moreover, in complex socio-technical systems – like systems which would interact during a large-scale cross-border disaster response – roles and responsibilities of individuals overlap and new risks that are beyond individual responsibility arise, making it hard to leave the responsibility to individuals along the way to perform assessments of risk and ethical impact of their work, as each individual cannot entirely see their relation to the whole system in which they act (Perrow, 1984; Vaughan, 1996). Consequently, ELSI cannot be left to the users alone, but also need to be considered in the design and organizational contexts of the technology itself and how these encourage different forms of use and enable practices.

To address these complex challenges, this document provides three things: 1) an elicitation of ELSI that need to be addressed in the design of a complex socio-technical system for information exchange in disaster response; 2) a first draft of human-centred collaborative research methods that will help derive, address, and manage ELSI throughout the design process; and 3) an initial list of ELSI qualities to consider in the non-functional architectural qualities of SecInCoRe. To do so, it draws on a range of sources, including previous literature, similar information exchange projects, data from case studies within SecInCoRe's preliminary inventory, and data from a first co-design workshop and a pilot questionnaire sample. While it is impossible to foresee all situations in advance, by considering ELSI it becomes possible to pose questions of our design process that can help make the underlying socio-cultural structures and contexts that influence decision-making and information sharing practices more visible in ways to produce "good" technological progress.

2.2 How SecInCoRe thinks about ELSI

There are persistent calls for more effective collaborative practices in emergency response (ENISA, 2012). These practices require organizational and technical interoperability, including extensive and intensive exchange of situational information, existing knowledge, as well as translation between diverse organizational and situated practices. To do so requires knowledge of the different stakeholders, perspectives and expectations that will comprise the emergent practices and conventions of inhabiting the information space. Addressing ELSI must balance the traditional exploration of

values and norms that structure decision making with the need to be inter-cultural and interdisciplinary in order not to perpetuate social power-struggles, injustices, or culture-clashes (von Schomberg, 2007).

ELSI is central to SecInCoRe in four ways. First, as designers of a new architecture for collaboration and data sharing for disaster management, we take on specific ethical and social responsibilities as stewards to those we aim to serve with the final product. Second, considering ELSI brings the user into the design, acknowledging how sense-making comes from using technology, not from the technology or the user alone. Third, addressing ELSI can help balance the individual with the collective, the user with collaborative practice and institutional context. Forth, the public's acceptance of emergency response actions in general is intertwined with ELSI: if the actions of the responders are not understood as ethical or trusted as legal by the public, then the public loses faith in the response.

As we design a tool to aid in information sharing and storage for use in emergency response, we become co-stewards of the welfare of the data and the public interest being aided by our tool. Our designs should support data stewardship. Similar to land stewardship, this stewardship is about the long-term maintenance of data that safeguards diversity and authenticity as the data is held for future generations and managed based on their interests, not ours (Baker & Bowker, 2007; Egan, 2011). The public has the right to demand managerial and regulatory commitments from those who take on a stewardship role regardless of whether such commitments are achievable (Egan, 2011). In order to gain and maintain public trust and confidence, stewards must be aware of the public understanding of their practices and solutions and the extent to which their practices and solutions make the public vulnerable (Jasanoff, 2010).

This awareness can come from considering ELSI. However, ELSI only appear when the technological practices are socially, culturally, and institutionally situated. Without considering how, when, by whom, and to what end a technology or related practice gets used we cannot understand the socio-cultural forces that influence the design process to begin with (Feenberg, 2010). While it is possible to design a disaster information sharing system that asks "will you use this data ethically (y/n)?", a basic Boolean function, the answer to the question cannot be reduced to the rules of that function. The meaning of those rules – the true/false nature of the question – have implications beyond what can be outlined in procedures or what can be structured into software and hardware (Woolgar, 1990). They are shaped not only by who is answering, but also by the characteristics of the hazard faced, the scale of emergency, the context of action, and the practices of those responding. Moreover, once in practice, these systems can have unintended consequences as to the behaviour of their users, structuring the possibilities for action and understanding, and thus how the user makes sense of a situation.

For instance, tools for aid distribution often draw upon local demographics to help determine how to spread the resources. However, if those demographics are used to create a classification system and then applied to another region, they might not only be found as irrelevant to the needs of those being served, but they could lead to new forms of judgment, social sorting, or barriers to aid for groups not included in those demographical categories or that classify themselves differently. This happened in the

U.S. during the 2010 census. Citizens of Mexican heritage, who accounted for more than half of U.S. population growth between 2000 and 2010, could not find a racial category on the survey that fit their understanding of self. Instead, they had to classify themselves as “white” or “some other race” for which each individual created their own definition (U.S Census Bureau Brief C2010BR-04). The fact that they did not fit into the classification schema diminished this demographic groups’ presence and thus socio-political influence. As socio-technical systems become more complex, they can accommodate more details to help alleviate some of these issues. But at the same time, the more complicated the systems get, the greater their reliance on experts, the more alternative ways of knowing are rendered subordinate or dependent (such as Mexican immigrants’ understanding of race versus U.S. government’s understanding of race) discouraging joint responsibility, distributed justice, and democratic participation (Egan, 2011; Mahony & Hulme, 2012).

Nor is this limited to classification systems within technological design. Social effects of technological design can also been seen in system architecture. For example, Latour (1992) points out how a speed bump or an automatic seatbelt force certain behaviours onto car drivers (slowing down or buckling up). While in most cases such behaviours are generally designed for the safety of society – it is considered “good” not to drive too fast and is “good” to wear one’s seatbelt – they do not leave room for exceptions, like the ambulance trying to get to an emergency for which the speed bumped road is the shortest route - it either has to slow down as it goes over the speed bumps or take an alternative, longer, route. Either way, the speed bumps force it to arrive later to a scene of medical need where time matters. In another example, it is a general rule that keeping data private and secure is good, but there are moments when sharing that data to save lives is more important and equally ethical. Again, just inserting rules into a system is not enough to address the potential ELSI that arise. The question for SecInCoRe becomes not how do we define privacy or surveillance, but who will decide, why, to what effect and – critically - how? This moves us away from any simple possibilities to enforce privacy by design (Cavoukian, 2001, 2012; Langheinrich, 2001) and towards the need to design *for* complex privacy practices (M. Büscher, Perng, & Liegl, 2015; Dratwa, 2014; Weitzner et al., 2008).

The methods and guidelines presented in this document are intended to help uncover and question these taken-for-granted forces in order to develop a more ELSI-conscious design process. The methods and guidelines are also designed to aid in foresight and knowledge assessment, providing questions we should be asking of the SecInCoRe components in order to be aware of the ethical, legal, and social implications of specific design decisions.

3 Previous Literature

3.1 Emergency Ethics

One of the primary debates in emergency ethics is whether emergencies should be considered *exceptional* situations and hence warrant responses which in times of normalcy would be considered unethical or illegal. These debates shape multi-agency emergency response in significant ways, with questions like:

- Does the end to save lives (resources or public order) justify the means?
- Does an emergency justify suspending fundamental human rights?
- If an emergency makes it necessary to violate certain rights, what should be the thresholds for these exceptions and their limits (scope and duration)?
- How much investment of time, energy and resources in preparation should be expected to avoid the need for exceptions, and how should the costs and benefits of such preparation be distributed?

These ideas originate with Schmitt (2012, orig. 1922), who couples the concept of sovereignty with that of exception. This relationship between exception and state has been expanded by later scholars to include the idea that governments or heads of state should be entrusted with the authority to make decisions (Sorell, 2003; Walzer, 2006).

However, other ethics scholars challenge the view that a state of exception should place state and society outside normal law and morality. For example, Ignatieff (2005) argues that exceptions can set dangerous precedents (citing examples such when the Bush administration used military tribunals to try terrorists rather than putting them through the federal court system), Coady (2004) criticizes both conflating a state's survival with that of its political leadership and suggesting that exceptions are hard to distinguish from terrorist acts, and Sandin and Wester (2009) suggest that the notion of exception relies on the myth of disasters as times of moral black holes that threaten a breakdown of social order. Demonstrating the uncertainty of emergency ethics, Green (2007) shows the moral and legal complexities of 'good' and 'bad' looting during disasters, and Murphy and Whitty (2009) discuss the problems of considering public health emergencies as security threats.

Legal discourses often centre around whether emergencies can and should be governed by the law, or whether emergency powers outside of the legal framework or constitution should be granted. Finding a balance between effective disaster response, constitutional principles, and emergency powers, includes the challenge of balancing upholding the rule of law and protecting human rights. Three main branches exist (Dyzenhaus, 2006; Ferejohn & Pasquino, 2004; Zuckerman, 2006):

- *Monist position*, which rejects the idea that emergencies justify any alternation in the ordinary scheme of governance;
- *Dualist position*, which advocates the construction of a legally authorized space of discretionary power in ordinary law, designed to guard against a breakdown of the norm/exception dichotomy;
- *Schmittian position*: as we saw before, this promotes the view that an exception should exist outside of the law making it impossible to apply normative judgement to the state's actions during an emergency.

The debates between these branches bring into sharp focus the tension between security and human rights considerations, especially when different countries adopt different stances (Scheppele, 2006) or when trying to synthesize emergency power and liberal democracy (Scheuerman, 2006). For example, Scheppele discusses the significance and implications of the US's Schmittian attitude towards the use of emergency powers, which continue to be felt worldwide, long after the events of 9/11, when President George W. Bush declared a "global war on terror" allowing him to assert extraordinary constitutional powers and then invoke an all-powerful commander-in-chief clause in the U.S. Constitution for justification of these powers (234: 22). It broadens the concept of war, blurs the boundaries between legitimate or illegitimate use of extraordinary powers, and leaves open the question of the role of the military on domestic territory.

Questions regarding emergency powers and the role of the military are not restricted to cases of terrorism but also concern civilian emergency situations like natural disasters. These are questions such as: if natural disasters bring about violence and looting in people's struggle for survival, or if criminals take advantage of disasters, what means can the military use in order to uphold order? Also, what happens when the chains of command become unclear affecting the interaction between agencies? Dougherty (2008) argues it was not the PCA - *Posse Comitatus* Act (which prohibits the use of the standing military to execute laws) that delayed the formal response to Hurricane Katrina leaving those affected without aid for days, but rather ineffective government administrative and emergency management. The argument for a multi-disciplinary approach to improving governance is a theme that runs through the volume. For Waugh and Streib (2006) a key issue in the Katrina response was the lack of situational awareness and flexibility in the command and control model of the Department of Homeland Security. They cite the need for innovation, adaptation and improvisation. Overall, the arguments point to the need to focus on factors beyond just the legal – be it operations, technological, or political – for effective emergency management.

Debates on *what* is an emergency, *who* has the authority to define it and *which* emergency measures are justified in which situations matter to the ethics of IT supported multi-agency emergency response as they bring into focus the importance of having as accurate as possible dynamic risk assessment and communication during the response phase. Yet this scholarship does not go far enough in considering the *how* of ethics in emergency management: While these debates are important they leave underdeveloped how ethical principles, legal rules and social values are embodied and practiced, in context, by emergency responders, individuals and groups affected by emergencies. There are empirical studies (Hoffman & Oliver-Smith, 2002; Kendra, Wachtendorf, & Quarantelli, 2003; Quarantelli, 1994; Rake & Njå, 2009; Stallings & Quarantelli, 1985) and, on an organisational policy level, many professional emergency response organisations, NGOs and associated professions have devised ethical and professional codes of conduct. These range from humanitarian principles to guidelines for disaster risk reduction, ethics of teamwork and multi-agency collaboration, and specific guidelines for information sharing in conflict situations (for a review see Monika Büscher, Liegl, & Wahlgren, 2014; HM Government, 2013; International Committee of the Red Cross, 2013; Prieur, 2009). Many studies show that extreme events require both planned and improvised responses, involving

established as well as ad hoc organisations, and 'emergent interoperability', a fact of disaster response that needs to be addressed in relation to ELSI (Harrald, 2006; Mendonça, Jefferson, & Harrald, 2007). There is also a growing body of work with an interest in virtue ethics in disaster response (Franco, Flower, Whittle, & Sandy, 2015; see Jennings & Arras, 2008; Larkin, 2010; Zack, 2009). However, while these studies and codes of conduct discuss what *should* be done, they only begin to address how is ethics *practiced* and *how* can societies do better?

This is especially important to understand for technological innovation. Yet, the role of technology in shaping emergency response is underdeveloped in the academic literature that focuses on emergency ethics, even though technology has always played a central role in emergency response. From fire-fighting equipment to incident command systems and the recent proliferation in digital technologies, technology has shaped responders' abilities to act, communicate and coordinate, to carry out risk analysis and to gather and process information about an emergency (Buck, Trainor, & Aguirre, 2006; Moynihan, 2009; Muhren & Van de Walle, 2010; Ramirez, Buscher, & Wood, 2012). For example, Jillson (2010) discusses ethical opportunities, such as the capability of emergency management information systems (EMIS) to extend surge capacity, to maximize availability and enable more equitable distribution of services, and to enhance risk communication. But she also shows how the informational and communicative advances that EMIS can enable and can complicate adherence to core ethical principles of non-maleficence and beneficence, respect for human dignity, and distributive justice (equal access). Büscher *et al*. (2013) demonstrate that EMIS can both exacerbate problems regarding the loss of privacy or the normalisation of surveillance (see Norris, 2002), and also contribute to new, more efficient forms of communication, coordination and collaboration through a focus on 'emergent interoperability' (Mendonça et al., 2007) and innovative approaches such as 'privacy by design' (Cavoukian, 2001; Langheinrich, 2001).

Recent developments in ICT technologies have also led to the mobilizing of new publics during emergency situations, for example the use of Twitter in allowing instant notifications and dispersal of information (Rizza, Pereira, & Cuervo, 2013; Starbird, Palen, Hughes, & Vieweg, 2010), and the formation of 'digital humanitarian organisations,' such as CrisisMappers, Standby Task Force (SBTF) or Humanity Road. These new globally distributed digital volunteers are gathering and mapping information from afar (M Büscher, Liegl, Perng, & Wood, 2014). These developments raise many new ethical, legal and political opportunities and challenges and there is an emerging body of research that has begun to explore these issues (for example Latonero & Shklovski, 2011; Palen, Hiltz, & Liu, 2007; Shanley, Burns, Bastian, & Robson, 2013; St. Denis, Hughes, & Palen, 2012; Tapia & LaLone, 2015; Watson & Finn, 2013 among others). Considering how the introduction of new technologies and technological practices are intertwined with the core understanding of disaster (e.g. what would make a state of exception) and disaster response (e.g. who is responsible for responding to help who?) will open up the space for more appropriately addressing ELSI issues, such as privacy, security, liberty, as well as a deeper understanding of their interaction.

To help elaborate on these issues, this chapter draws on scholarship that explores the relationship between user and technology, the ethical implications of using rule-based systems, and the interconnections between socio-technical futures and collaborative

practices. For an effective approach to considering ELSI in the design of a socio-technical system for information sharing during emergency response we need to ask not only how institutions and people can act virtuously in crisis, but also examine how technology can be designed in ways that support new practical ethics and virtuous conduct.

3.2 Users and Technology

Studies of technology and their users have demonstrated that technologies do not exist independently from their situations of use. Technologies are made sense of by the meanings we give them – through design and use – just as much as the programming and structures they provide (Feenberg, 2010; Woolgar, 1990). They are what they are made of *in situated action*, not something innate to their design (Suchman, 2007). Some go so far as to suggest that the same physical apparatus is a different technology when put to different use in new contexts (de Laet & Mol, 2000). In this way, people interacting in the world are central to the design process, not just the engineers doing the designing and the technical systems being designed (Dourish, 2001).

The argument also works in another direction: we do not “use” technology to know the world around us, per se, but technology is implicated in what we consider knowledge of the world to begin with (Hutchins, 1995). As we engage with technologies to learn more about events or issues, they do not just enhance our vision by creating lenses with a finer resolution of information, but help shape how we think about the issues and events. In other words, specific understandings of situations and communication cannot be recreated through the rule following upon which technology, software, and their system architectures are built. This kind of sense-making happens through how the rules are put into practice towards specific goals (Wertsch, 1998). For example, while all chemical containers in Finland are supposed to be labelled with their contents, in practice this is not always the case. There are no rules that can be written that can guarantee an understanding of when the contents and labels do not match and to tell us when that mismatch is significant. In this way, day-to-day usage, rather than exceptional, need to be considered in the design so that these local and tacit aspects of use and rule following are accounted for (Turoff, Chumer, Van De Walle, & Yao, 2004).

For example, during an emergency in Finland when a mislabelled chemical tank was found smoking and potentially leaked hazardous materials, the officers at the scene found that no pre-determined practice or technological gadget could get them the data they needed to determine the extent of the hazard; only through the use of technology in that specific context were they able to grasp the implications of the mismatched label and contents for their response. What they needed to know was partly a function of the situation and location, day-to-day experiences, the expertise available at the scene, the historical knowledge accessible, and the technological tools they could use. No single ingredient could determine what should be known without the other elements – no clear rules could be written or designed in advance to structure the necessary data.

Considering emergency ethics, then, requires an open examination of the role of technology-in-use in disaster response. Understanding how a technology is and could be incorporated into sense-making practices is vital to any interoperability because

they shape terminology, interpretations of data, priorities, values, what is considered acceptable accuracy or actionable information and decisions that result from the data use. Considering IT ethics during disasters means thinking about how the IT is used rather than just theoretically what the IT makes us capable of doing.

3.3 Standardization, Classification, and Ethical Practices

In order to share data across borders – be it between agencies, jurisdictions, or nations – there must be some data standard (even if ad-hoc) in order for the various technological systems along the way to be able to incorporate the data during and after the sharing process. However, standards and classification systems are codifications of value systems and social practices. They are not ethically neutral tools for organizing information, but ways of normalizing specific ontologies and social orders. Their use alone brings up a range of ethical questions.

First, standards for data sharing carry with them value systems. Standards and classification systems are designed to enable and maintain formal order, including standardized communication networks, terminology, data gathering routines, and mapping systems. But while they make shared action possible, they also carry in their conventions the norms of society, value systems that are situated in specific events, places, and times, as well as the work being asked of the data (Bowker & Star, 2000; Fiore-Silfvast & Neff, 2013). For example, working with specific geographical framing mechanisms, like those used to structure GIS data, affects how the causes and effects of a disaster are identified and what elements and people are considered to blame (Frickel, 2008). The different structuring frames presented by such organizational conventions can change whether the 1984 Bhopal disaster[1] is an Indian only disaster to be dealt with internally or an international disaster with responsible parties spread as far as the United States. Changing the classification framing mechanism can change whether disaster recovery is considered complete or still on-going or whether what is relevant to consider are immediate chemical spills or future health problems (Fortun, 2001). Through their use, classification systems and related technologies produce and perpetuate specific forms of social engagement as well as understandings of the areas affected and people being served

Archives—such as inventories of disaster events, ELSI, data sets, command systems including information management processes, information systems and business models—act similarly. Such inventories have been identified as necessary for producing new information on expertise and necessary resources (Rademaekers, Eichler, Holt Andersen, Madsen, & Rattinger, 2009). Yet, as Fritzsche (2005) argues, archives enable us to engage with data in ways that *produces* rather than *describes* histories. The status of data in an archive is not innate to the data nor the incidents being represented. The histories saved into the archives come from those doing the recording and organizing of the data into standard formats and shared classification systems (White, 1978). An inventory, even if it is constantly growing and changing shape, is a set of elements assembled for a reason, where the work of recording an

[1] In December 1984, a Union Carbide India Limited (UCIL) pesticide manufacturing plant leaked a mixture of toxic gases, killing between 2-4000 people in the immediate aftermath and significant long term health effects for hundreds of thousands (Fortun, 2001), classed as one of the worst industrial disasters in the world's history.

(on-going or past) event makes “meaning by choosing and placing and pasting” elements together in relation to one another, circumscribing and delimiting meaning through these relationships (Smith, 2004, p. 7). The relationships created for these elements in an inventory have ethical implications, especially in relation to inclusiveness and neutrality, for how the incidents become knowable.

For example, Sekula (1986) finds that in the act of filing photographic documents of prisoners into a cabinet it is possible to see value-laden and situated nature of classification. For example, one way to file such data is to allow users to sort by specific crime, offering a particular, but isolated, event for inspection. Another is to offer a sampling of events that are typical or emblematic of a specific feature, offering “representative” instances. One provides a specific person, the other an “average” prisoner. One offers particular details relevant only to a specific context, the other creates an “ideal” and a “normal” type of prisoner. In the context of disaster management, looking at regional averages in order to determine civil protection needs (as suggested by Rademaekers et al., 2009) provides a way to think about distributing resources, but at the same time is also produces socio-political norms.

The different relationships and extrapolations drawn have strong ELSI implications for how the data in such systems gets used and is made sense of. Bowker and Star (2000) note that knowledge about what is useful at any given moment is embodied in social roles and the accompanying mundane practices. When different roles meet, these practices appear less mundane and the assumptions behind them can no longer be taken for granted, highlighting the exceptions to the standards or where the classification system breaks down. Consequently, carrying a standard or archival practice from one place to another or one situation to another is an act of imposing one set of values onto another as well as acts of potential limits to data use.

If standards are treated as boundary objects, that is objects of common concern that may have different meanings for each group engaging with it but that are recognizable as common, some form of classification system is necessary. But this cannot be imposed upon the practice from the outside; it has to come from within the practice (Star & Griesemer, 1989). For example, e.g. a triage form or a medical record means different things to paramedics, nurses, doctors, or social services personnel, yet they can all enter information into such a form or record in ways that would be useful for all others and more or less uniform.

Classification systems and standards pose a few other challenges. First, as disasters disrupt daily routines, they make it difficult to maintain any classification systems or related standards, especially as disasters constantly make room for questions about what defines the order of the everyday (Steinberg, 2000). Second, classifications only work if they maintain an awareness of local variations. For something to be a standard, especially when dealing with multi-agency or distant collaborations, it has to be able to accommodate diversity in practice (Edwards, 2010; Jordan & Lynch, 1992). Coordination between diverse groups cannot occur if there is not flexibility within the conventions for managing local issues, something necessary for improving EU coordination during crisis response (Rademaekers et al., 2009). If a set of rules or instructions cannot accommodate different circumstances, then it cannot be used in multiple locations and thus will not become a standard. In addition, the localized nature of the standardized practice often appears in an expert’s inability to describe

procedure in a way that separates out the standards from the personal (Jordan & Lynch, 1992).

In their work on building diverse information databases for ecological knowledge, Baker and Bowker (2007) suggest that when working at the intersection of multiple ontological frameworks, the challenge becomes one of determining what type of knowledge gets included into standards and systems of classification in ways that keep diversity and ambiguities with the data. They build on the notion that any incident has to negotiate internally three different types of knowledge: tacit, background, and rule-based knowledge. Included with these are the tensions between knowledge that is derived by the different groups working together that needs sharing. They find that some of this knowledge cannot be reconciled technologically with rules or via shared standards, but needs constant “intermediation” by liaisons. This is especially the case if there is to be any long-term maintenance and preservation of the data, where data diversity increases with time. The question becomes how to keep the ambiguities in the data and the diversity necessary for encouraging broader views and balancing these, while simultaneously creating a shared, intersubjective vocabulary of action. These issues all demonstrate a need for translation, yet offer no specific solution to this.

3.4 Sociotechnical Futures and Collaborative Practices

Innovation in information sharing during disasters can offer great social benefit. It can enhance risk awareness, preparedness, the speed and efficiency of response, support people in complying with legal obligations, and encourage a greater awareness of how different groups make sense of unfolding crisis situations. In doing so, it can enhance the humanity of disaster response and management, by putting people, their needs, feelings and relationships more firmly in the centre of the work that needs to be done to prepare, respond to, or recover from disasters. However, such innovation can also engender problematic transformations, as it increases public visibility and accountability for emergency responders, produces challenges of controlling accuracy of information, including rumours, requires management of vigilantism, problematizes data protection and privacy issues, and adds frictions to practices of organizational information politics (Monika Büscher, Liegl, Rizza, & Watson, 2015; Crowther, 2014; Jillson, 2010). Such transformative consequences arise in everyday practice, often in unintended ways. For example, with novel information technologies, all emergency response communications can be logged – such as the police communications during the Boston Marathon. When records like the police scanner come into the hands of the media or social media, they can become resources for real-time analysis by ‘issue publics’ such as that mobilized by the FBI as they requested a public hunt for suspects of the Boston Marathon bombing. It can become very difficult to control the spread of information in such situations (Starbird, Maddock, Orand, & Achterman, 2014; Tapia & LaLone, 2015). The transformative consequences are unknowable in sufficient detail in advance of actually taking new technologies into use (Suchman, 2007). Thus IT innovation constitutes ‘disruptive innovation’, that is innovation that spreads in positive and negative ways across economic, social, political contexts in ways that cannot be anticipated (Chesbrough, 2003). It is impossible to gain a sufficiently rich understanding of different stakeholders, perspectives and expectations that will

comprise the emergent practices and conventions of information sharing through studies *of* potential users and use contexts alone or by exploring the technology alone.

Collaborative design can help make visible these otherwise unknowable consequences. It is a methodology that involves the people who will be affected by new technologies throughout all design phases. It brings into one conversation multiple perspectives, forms of expertise, and contexts, as it explores the interplay between the social, technological, and organizational through hands-on engagement with prototypes. Co-design is a way to study emergent technologically augmented practices *in vivo*, making technology's workings—including breakdowns, frictions, and opportunities—visible as an on-going practice (Bellotti et al., 2002; Introna, 2007). Co-design also makes it possible to treat 'user needs' and design solutions as co-emergent and dialectical. How a problem is expressed, what elements become part of the solution, and an individual's capability to solve the problem change based on the context of interaction, visions, opportunities, and practices and are impossible to foresee by a designer in advance (Dourish, 2001; Lave, 1988). Participants become a collective resource for design and produce an environment of mutual learning (Törpel, Voss, Hartswood, & Procter, 2009). Co-design thus facilitates both *discursive* and *practical* co-realization of socio-technical futures (Hartswood et al., 2008). While in this context there are some parameters of SecInCoRe that we will not be able to manipulate through design, such as Information Systems, through these methods we may be able to discuss the functionalities and possible information that should be incorporated and made available.

For SecInCoRe will draw upon co-design to provide insight into ELSI as they arise in emergent socio-technical futures in disaster response and management. To do so, we are pairing these practical engagements with disclosive ethics investigations, which involve a tracing of 'effects' that technologies-in-use engender for different stakeholders (Introna, 2007), to pair the envisioning of new potentials for innovation with the uncovering wider more 'disruptive' aspects of innovation as they emerge (Chesbrough, 2003). In this way, ELSI become concrete matters of concern, and open up opportunities for innovation during all phases of technology development and use, including conceptualization, production, and implementation (Monika Büscher, Simonsen, Bærenholdt, & Scheuer, 2010; Ehn, 2008; Hertzum & Simonsen, 2011; Liegl, Büscher, & Oliphant, 2015). In this project we hope to address positive and negative unintended consequences throughout the design process instead of after-the-fact.

Developing collaborative methods is also important because they make it possible not just to incorporate new practices and technologies into user practices at present but to also envision what might happen next. Working alongside users enables creative anticipation of emergent future practices that can inform both more 'appropriate' and more ambitious innovation. It also enables designers to engage with the qualitative aspects of disaster response, valuable knowledge since much of the data gathered about an incident is qualitative in nature, such as textual or image (see D3.2). This is important, as new technologies often emerge and evolve along with transformations in practice (Callon & Muniesa, 2005; Haythornthwaite, Lunsford, Bowker, & Bruce, 2006). In addition, different cultures of practice integrate digital infrastructures in historically and culturally specific ways, giving the same architecture unique functions for different practices (Merz, 2006). Envisioning how such transformations might occur is useful to

enable a successful incorporation of such visions into daily practice (Hertzum & Simonsen, 2011). Incorporating visions of the future into disaster research is important because in many ways, it is the anticipation of future events that drive present practices (Jasanoff, 2010; Lakoff, 2008).

3.5 What this means for our methodology design for human centred research

A close interaction between designers and users is required for a result that will benefit all stakeholders, especially first responders who increasingly face situations where collaboration with other agencies is required, during an emergency. But to encourage such collaborations, we need to begin with a careful selection of criteria necessary for decision-making and response management, including nuanced definitions of crisis, information and data and the sharing of these, that will lead to decision-making as well as management. While it is possible to gather some of these details, such as lists of crisis management models and information systems, this information alone does not dictate what happens during collaborations and how the ethical issues implied in these various criteria are embodied.

Working collaboratively, users (both of previous practices as well as early adopters of SecInCoRe's new tools and procedures) can provide valuable input for the information, social and technical functionalities that are critical during an operation, while designers will provide insight into the feasibility and specificity of features that can be made available for the users. While it is possible to gain information about users perspectives from questionnaires, workshops, interviews, etc., it is not possible to forge new unforeseen paths, to innovate in ways that rethink problems in new ways. For this, the users and designers have to work together at all stages of the design and actually build and experimentally implement prototype (assemblies of) technologies. This way it becomes possible to learn about how a feature could be used in practice, not just discuss what the feature is capable of. It also becomes easier to separate the localized and personalized touch of practice from the standards of procedures upon which those practices are based.

For collaborative methods like this to work and produce results that are relevant to operations that are cross-border, the users participating must be drawn from all of the agencies involved during operations, and it must include engagements with SecInCoRe's prototypes. This engagement is important because it gets at the how, not just the what. With the switch, the explanations often change. For instance, in engagements with first responders and police authorities in previous workshops several obstacles in sharing data and information were identified, but only after the interactions moved to how data sharing would be done, beyond just exploring what might be useful if it could be done. For example in a stakeholder based workshop for the project EVA (https://www.cik.uni-paderborn.de/en/research/public-security-safety/eva/) potential end-users were asked to test the potential usability of a web-based system for planning safety and security during a major event being designed. These users, ranging from first responder organisations to police authorities, all agreed upon the benefit of such system for reducing planning coordination between different organisations. When asked "is this usable?" they said 'yes'. However, when asked to demonstrate how it would be useful, the participants became sceptical and hesitant. It turns out they all had great uncertainty regarding the legislation of data sharing. They did not know which data was sharable and which was not. In addition,

some of the participants refused to use the system because they feared that their inputs into it might be used later to prove that they have made a wrong decision or did not follow guidelines or regulations. Or worse, that it changed the question of responsibility for the data security: was it the system, the person who used the data, or the person who entered it? These types of ELSI are at the heart of usability and viability. They cannot be derived from listing rules or answering questionnaires.

4 Study of interfaces to other data sharing and information exchange projects

While looking at the academic literature that engages with ethics, IT, and standards in relation to disaster response and management is central to our work, it is also possible to draw lessons from research in other contexts where interoperabilities and interfaces of similar complexity and scale are needed. Looking at these is useful to understand user goals and socio-technical futures, what they suggest about ethical issues to be encountered in such systems (not just within the data), as well as to understand how to think about human-centred collaborative research methodology.

4.1 Smart City Endeavours

In the past four decades, a vast body of literature has discussed the installation, application and influence of digital and electronic technologies within cities in order to better gather and share data about activities within city boundaries (Hollands, 2008; Kitchin, 2013; Townsend, 2013). This literature has labelled digitally and electronically augmented cities as 'intelligent', 'wired', 'cyber', and most recently 'smart' (Hollands, 2008; Nam & Pardo, 2011). As Kitchin (2014) and Godspeed (2014) explain, there is little consensus amongst academics, technology companies, and public administrators about what it takes to be a 'smart' city; is it a city that uses technology to overcome rapid urbanization challenges (Washburn et al., 2010) or simply a marketing term (Greenfield, 2013)? The technologies and infrastructural architectures themselves are not enough to define the meaning and purpose of such systems, even if they have created a base upon which to build.

Within this broad 'smart city' discourse sits a discussion about how 'smart' cities can respond to disaster and emergency situations. Some academics and public administrators have claimed that technologically advanced cities will be more 'resilient' and prepared to respond to disasters as a result of the additional technological systems (Godschalk, 2003). Technology companies have produced a significant amount of literature claiming 'smart city' technical solutions will improve emergency and disaster response times, logistics, services, and speed up recovery. For example, IBM's states:

> *'Organizations worldwide have found that Smarter Cities® emergency management solutions can help mitigate potential events, prepare for future threats and adverse events, respond professionally to those events, and quickly return the community to normal'* (United Kingdom Department for Business Innovation and Skills, 2013).

And Motorola promote a similar vision:

> *You can't predict what you don't know or can't see. Turn relevant, timely information into intelligence so you can act. Our system goes beyond just simply collecting and aggregating data; we'll help you leverage advanced analytics so your staff can more effectively assess that data to better anticipate, forecast and predict incidents and potential impacts for a more proactive response* (Motorola, 2012, p. 5).

This 'smart' emergency response presupposes, places technology and data at the heart of efficient response, claiming to form one, real-time view of incidents so as to establish 'a unified operational view' for all involved agencies (Motorola, 2012, p. 5).

These claims are not limited to for-profit companies and governments. Technologies developed and deployed by small start-up companies and non-profit 'digital humanitarian' organisations, such as Ushahidi, the Standby Task Force, and the Humanitarian OpenStreetMap Team, are also often linked to improving 'smart' disaster and emergency response (Humanitarian OpenStreetMap, n.d.; Meier, 2012).[1]

However, many challenges have also been identified to achieve these goals, inciting arguments against relying too heavily on technology during disaster response (G. Graham, 2014; Greenfield, 2013; Mullagh, Blair, & Dunn, 2014). In particular, Allen, Karanasios, and Norman's (2013) research highlighted the organisational and cultural challenges that affect disaster response organisations, suggesting focusing on interoperability as a primarily technological issue will not solve the problems faced. Rather, interoperability is an organisational and informational issue that needs to be addressed for any technological solution to work. This is a challenge that numerous EU projects are currently addressing, including DITSEF, IDIRA, CRISYS, ESS, HIT-GATE.[2]

Others express concern specifically about the disaster environment, especially the relationship between technological systems, the often improvised and hastily formed networks created with them during the disasters, and the need to reconfigure them to function during the fragile post-disaster environment (Nelson, Steckler, & Stamberger, 2011; Yan, Qian, Sharif, & Tipper, 2013). This can be aggravated if the citizen's understanding of the situation and the technological solutions clash. For instance, what if locals will not leave a flooded area as directed? Or what if locals are prevented from evacuating even if their lives are in danger? This leads to the question: Are 'smart cities', and their hardwired structures, truly more prepared for and resilient to disasters than non-'smart cities'? Are citizens actually smarter as a result of the connectivity or does the structured nature of the smart-city limit possibilities for knowing? What happens if a smart city environment (or network) breaks down, like in the case of a blackout? Moreover, however well-prepared, any sociotechnical system can suffer full

[1] These digital humanitarian organisations are based in volunteers spread all over the world, frequently having no direct connection to the places affected but stepping up, via networked connections, to offer help however they can technologically (such as mapping or translating text requests for help). The notion is that humanitarian aid can come in the form of networked data sharing. www.ushahidi.com, blog.standbytaskforce.com, hot.openstreetmap.org

[2] DITSEF: http://www.ditsef.eu/ "Digital & Innovative Technologies for Security & Efficiency of First responder operations". Aims to help interoperability through the design of self-organizing, ad-hoc communication systems that include enhanced geo-position and visualization sensors.

IDIRA: http://www.idira.eu/ "Interoperability of data and procedures in large-scale multinational disaster response actions". Aims to help interoperability through the design of "a technological framework covering recommendations for operational procedures and a set of fixed, deployable and mobile components including data and voice communication".

CRISYS: http://www.crisys-project.eu/ "Critical response in security and safety emergencies". Aimed to help interoperability through the design of a scalable crisis management system that focused on collating capabilities and domains into a systems of systems.

ESS: http://cordis.europa.eu/project/rcn/91016_en.html "Emergency Support System". Aimed to help interoperability through the design of a "network enabled command and control system", based in a suite of real-time data-focused technologies.

HIT-GATE: http://www.hit-gate.eu/ "Heterogeneous Interoperable Transportable GATEway for First-Responders". Aims to help interoperability through the design of "a novel technological solution that will interconnect all the existing communication systems via a dedicated node."

or partial breakdown (S. Graham & Thrift, 2007). It can be sensor failure, less-than-desirable data quality, insufficiently trained algorithms. In these situations, it becomes necessary to consider what 'resilient' means, what it means to have 'enough' knowledge to act, and the delimitations of access. In other words, for the technology to offer a solution, it needs to be clearly aligned with the problem to begin with. In this case, the problems are not about getting people to talk but about aligning local meaning-making practices.

4.2 Lessons from Climate Science/Meteorology/Earth Observations

Climate and Earth observation systems have, for decades, dealt with large-scale techno-scientific data sharing. This sharing takes place over national boundaries, organizational boundaries, and physical barriers: in doing so they have encountered many ELSI issues that are relevant to SecInCoRe. Additionally, cross-national data sharing is of interest to data gathering during disaster response in general.

Weather services throughout North America and Europe have been dealing with interoperability of data for many years. To manage the weather and do long term climate models, data is needed from outside of national borders. In addition, the weather services often do not have the funding, staff, or the technology to gather all the data they need; to balance their limitations, they forge partnerships with research and private institutions to expand their resources. The groups involved all have different data gathering and storing practices that produce data that are neither at the same scale, resolution, frequency, or standards of accuracy. Consequently, the weather services have developed techniques for building into their data meta-information that is designed to help each group align the others without asking the others to change their cultures of practice. To aid in this process, some departments have created offices whose sole job is to support coordination (see, for example, http://www.ofcm.gov). These needs are not just for cross-border data exchange. For instance, in order for interdepartmental data sharing within the U.S., standards have been established for communication between agencies for regional meteorological information as well as environmental information during disasters, standards that include communications protocols, data formats, data storage and retrieval procedures, and data delivery/availability requirements. They also have spelled out methods for data aggregation and archiving. Included in these databases are the individual agencies' mission, authority, and responsibilities. In addition, each agency has established a memorandum of agreement that spells out specific obligations along that communication vector (Federal Coordinator for Meteorological Services and Supporting Research, 1998; Office of the Federal Coordinator for Meteorological Services and Supporting Research, 2010). Despite these initiatives, none of these procedures and technologies are expected to work or be useful without direct communication between the users (Federal Coordinator for Meteorological Services and Supporting Research, 1998).

In Europe specifically, sharing data between countries for weather has been commonplace, the first large committees designed to help create standards came to being in the 1870s. But despite a common interest and agreement for the need, it was also common practice only to observe agreements when they were useful, otherwise ignoring them (Edwards, 2010). Using these agreements strategically was also a way for scientists who did the intergovernmental work to keep some control and not lose

their autonomy as practitioners of science and be placed in positions as national representative, serving the interest of the nation rather than the scientific task at hand (Edwards, 2010). Another fear was the loss of diversity as meta-data becomes the standard for sharing, especially through the politisation of data sharing with standards designed from above/central bodies but meant to be enacted locally. Though it was scientifically agreed upon that there is no single appropriate approach to weather modelling, data sharing could force a single perspective upon the rest.

Some critiques are that meteorology, because of the public-private partnerships required to gather the extensive data, is becoming a political-economy approach that uses market-based criteria to allocate resources, or that the emergence of technologies created by private companies designed to improve data sharing but connected to profit-making (Randalls, 2010). For example, the need to work with airlines to get some of the atmospheric data has necessitated the public weather services to manage data selection in ways that are driven by commercial interests as well as scientific needs (e.g., the E-AMDAR programme).[1] Property rights issues have also played a role in limiting cross-border data exchange, as many countries offer different regulations on this account (Maurer, Firestone, & Scriver, 2000). In fact, even in cases of successful data sharing, rights to the data is held tightly: successful data sharing is often based on bartering credits and rights along with the development trust in what could be considered a 'gift culture' (Wallis, Rolando, & Borgman, 2013). These issues affect the quality of the data, how it is determined as accurate, and bring up questions about the privatization of what had been public goods.

4.3 Lessons from Crowdsourcing/Social Media

The advent of new information and communication technologies are altering and extending the way in which the public engages in and with disaster response, and even what 'public' is responding and why. How these technologies are changing the expectation of involvement, response, and responsibilities in public understanding of disasters have important implications for any new socio-technological system for information exchange in relation to disasters. Moreover, social media are increasingly resources drawn upon by first responders as they gather data about an incident, more so than data from NGOs, news media, or the general public (Co-Design Workshop 2014).

In some respects, the actual 'first' responders during disasters are often 'the public' who are at the scene or immediately connected to those affected (Alexander, 2013; Starbird, 2012). As a tool to both make more visible the public itself as well as what the public's role in response and recovery, social media and crowdsourcing tools are becoming increasingly prominent. These changes are especially seen through the mobilization of dispersed publics via crisis mapping (Liu & Palen, 2010) and via "blogs, micro-blogs, social book-marking, social networking, forums, collaborative creation of documents (via wikis) and the sharing of audio, photographic and video files" (Alexander, 2013, p. 718). Characterized by interactive communication, these forms of disaster response are intended to reduce community identified risks and response needs (Starbird, 2012). To this end, social media can act as a listening or monitoring

[1] s. http://www.eumetnet.eu/e-amdar

device for public sentiment, used for crowdsourcing and collaborative development, used for creating social cohesion in times of crisis, used to promote volunteerism, or simply as a way to communicate with friends and family when other communication technologies fail (Alexander, 2013; Liu, 2014; Starbird, 2012). While they are resources often drawn upon are not always easily reconciled with the official response plans and priorities because of the challenges balancing formal response structure with emergent cultural classifications (Liu & Palen, 2010).

One way in which social media has been enrolled in disaster response is through 'crowdsourcing'. While originally deriving from the term 'outsourcing' to harness "crowd power" (Yang et al., 2014, p. 2025), crowdsourcing commonly implies technologically networking and utilizing the distributed and collective intelligence of 'the crowd' to generate, organize, and manage information and solve problems. Crowdsourcing offers a unique perspective on interdisciplinary information exchange, providing insight into many of the grey ethical areas that any exchange system might encounter.

Gao *et al*. (2011) suggest various advantages to crowdsourcing in disaster relief. Crowdsourced data is timely; it can be collected almost immediately after a disaster has occurred through social media; crowdsourcing tools and applications (e.g. www.ushahidi.com, see footnote 1) are versatile and can collect data from various different sources (e.g. emails, forms, tweets, etc.). They also can act as classification tools, providing quick summaries, categorization, and analysis (via such methods as tag clouds, trends, filters). Finally, they can help with spatial awareness (through the use of 'geo-tags'). In addition, 'the crowd' can be used to validate information, as well as help to edit and manage information. These practices change the question from 'who' determines if data is relevant or meaningful to how the distributed system selects these qualities.

However, the increasing use of social media and/or crowdsourcing in disaster response also raises numerous challenges and ethical questions (see Alexander, 2013; Gao et al., 2011). While crisis mapping can help create increased situational awareness, there is still a lack of collaboration and coordination between response organisations and, thus, there is no mechanism to apportion response resources. There is also considerable debate about the accuracy or necessity of the information produced. Scholars point to the potential propagation of unintentionally or intentionally false information, raising the question of both organizational as well as public trust in regards to crowdsourced data (Starbird, 2011). This further raises questions regarding the decision-making practices of first responders who, in the event of relying upon 'unreliable data' may be seen as liable. There is also the concern of too much data and a lack of ability to adequately turn it into useful information in a timely manner.

But there are also deeper questions regarding who is 'the crowd'? And, following, what might this mean for creating biased situational awareness and, following, response? There is unequal distribution and use of social media technologies and applications within societies, for example along the lines of class, gender, 'race', age, disability, and skill (Alexander, 2013). Thus, while social media can, on the one hand, lead to a democratisation of voices, attention has to be paid to how this 'democratisation' is socio-technically structured, via "network capital" (Urry, 2007) and specific forms of literacy (Liu & Palen, 2010). The widespread use of social media in disasters, thus, raises the question as to how disasters may be socially (re)constructed through these

practices, by whom, and for whose benefit? Furthermore, while these forms of technological engagements may be a good source of information in the immediate aftermath of 'sudden disasters', its usefulness in drawn out 'slow moving disasters' or in the long process of recovery is open to debate.

The use of social media in disaster response also creates a 'wild information west'. Governments and first responders are less able to regulate or police social media and, thus, unable to control the public narrative, leading to not only the potentiality of false information but also to public panic. There is also the potential for these technologies to be used for criminal intent (e.g. terrorism) and, not unrelated, the openness of such platforms could also create new dangers to both first responders and victims (i.e. as their whereabouts become 'public knowledge').

Finally, there is the question of privacy. While Gao *et al*. (2011) suggest various technological fixes to the potential insecurities surrounding the use of crowdsourced data – such as: geo-tag determination through 'social mining'; using 'groupsourcing', or the collection of information through a delimited group as a supplement (helping create 'checks' on other crowd information); implementing verification buttons within systems (similar to the 'like' button on Facebook); the use of 'trust management systems'; the spatial-temporal mining of social behaviour prediction in order to 'fill in' information holes and gaps; and, the development of spatio-temporal classifiers for forecast models – each of these 'solutions' carries its own risks and, most notably, suggest making both potential victims and 'citizen reporters' more known and publically seen. Personal information, such as geographical location, name, etc., of victims and 'crisis reporters' may be shared via social media during times of disaster, questions arise as to what systems are in place to remove this information from the Internet after the disaster. Once this information has been shared – often with good intensions – how can it be unshared? How can consent be limited or revoked?

4.4 Border Surveillance

Emergency planning has been making calls against compartmentalisation and making a general call to think across boundaries which to manage the 'ever increasing interrelatedness and interdependence' of disasters (Boin & Ekengren, 2009). New forms of trans-boundary risks emerge (political, territorial, functional, time), where the boundary and the limits in data's ability to cross those lines shape the risk, not just the hazard that caused the need for the data movement in the first place. This does not mean, though that these cases are unprecedented or that the challenges they pose are always unique (Brändström, Bynander, & Hart, 2004).

One response is to argue that these new boundaries pose threats to the national safety and security. On that basis, "new security paradigms" are needed which see the European Union assuming a supranational and newly emerging security role (Boin & Ekengren, 2009). But a challenge here is the reluctance of nation-states, or organisations to cede authority, ownership, or control in key areas of the response leading to the fragmentation of response. Another response is to focus on how the local interfaces with the national (Jarman, Sproats, & Kouzmin, 2000), and to explore new multilateral governance structures that will operate on an international level (Boulden, 2004).

The ethical implications of these interactions are highlighted in situations of border surveillance. Border surveillance may enhance and extend state control over people within its borders, acting as tools of exclusion and repression. It can also act as a way to erase or undermine the border as the gaze of surveillance doesn't physically stop at the line (Walsh, 2010). For instance, if data gathering and sharing near a political boundary is considered a security threat, then any disaster along that line either forces the authorities on either side to make an exception to the rules of the line or it leaves a gap in what is knowable about the incident and given threats creating greater vulnerability in that region (Petersen, 2014).

In the European Context the debate around border knowledge has been around what crosses that space.

> *'…the rationale for strengthening of border control and establishing border surveillance technologies are bound up with the fight against transnational criminal threats such as terrorism, drug trafficking, and human trafficking and smuggling. A securitisation dynamic has thus been discussed with regard to the way in which the undesired form of human mobility known as irregular migration is re-framed in a European setting and placed on a continuum of threats alongside organised crime and terrorism — and against which practices of surveillance, control and penalisation are brought in or endorsed as necessary and legitimised.'* (Dratwa, 2014).

Such an attitude is a challenge to the EU backdrop of open borders and unification. While security is a human right, which type of security is it? Moreover, it puts into competition intelligence collection decisions and international trade negotiations.

Add IT to the equation, with such things as 'smart' surveillance technology, and the challenge becomes how to manage the incidental data that is gathered and what to do with the data that was gathered but cannot be exchanged due to the potential infringement of security and privacy rights (Kenk, Križaj, Štruc, & Dobrišek, 2013). Increased risks can develop for individuals of becoming the targets of law enforcement measures or secret surveillance, especially in the face of discrepancies in national reporting practices. However, responding to the discrepancies by interlinking the reporting has the potential to have one system, and its fundamental values, creep in and overpower another (Kenk et al., 2013). It also brings up a new problem: is security the responsibility of the state, of the technology, or of the citizens (Dratwa, 2014)?

5 The ELSI of information systems for data sharing and information exchange

An analysis of the previous two chapters, the results from the initial collaborative design workshop, as well as the case studies in the preliminary inventory from D2.1 (described as date, incident and/or country in parenthetics) leads to the identification of key themes in relation to how ethics, the law, and society interact with emergency response. While the issues are interlinked and the divisions between them somewhat artificial, and other categorisations are possible, the ELSI subsections here are designed such that explanations can be provided in ways that make possible productive action in design and practice.

5.1 Access and Equality

In the light of anti-discrimination provisions, the use of technology in crisis response needs to take into account inequalities of access at a number of levels:

- Reliance on a certain type of media, e. g., the Internet, can lead to societal groups being excluded from vital information channels (2002 - Prestige Oil Spill, Spain, and 2007 - San Diego Wildfires)
- Communicating key issues in a disaster situation, such as the need for emergency responders to inspect private homes for habitation safety, need to take into account a potential lack of access due to the event itself (1999 - Earthquake Athens, Greece)
- Questions of rights: who has the right to read, write, and delete?

The legal issues around antidiscrimination connect directly with questions about democratization, diversity, neutrality, and inclusiveness. How these issues are managed will affect the shape of vulnerability and justice.

5.2 Pre-emptive Risk Assessments

Inter-agency frameworks need to be developed that allocate responsibilities in relation to the communication of risk. These need to include pre-emptive duties with lessons learned from past events (2009 - L'Aquila Earthquake and 2011 - Bombing and Shooting, Norway described in D2.1). Connecting past to future, however, poses some ethical challenges. First, it potentially limits the versatility of the framework to handle new and unprecedented events or exceptions, something that is increasingly common in disaster response (Lakoff, 2007). Moreover, it needs to carefully consider the balance between learning from past events and maintaining inter-cultural and interdisciplinary values and norms in order to not perpetuate social power struggles or local injustices that emerged in those past responses. In addition, informational foresight is needed to understand when a situation is truly unprecedented or rare or when the challenge has been previously experienced but unnoticed (Brändström et al., 2004). Ethical foresight is needed in order to avoid perpetual piecemeal production of new legal frameworks after specific disasters.

5.3 Local and International Legal and Regulatory Changes

Many of the events illustrated in D2.1 and described in the 2014 Do-Design Workshop precipitate a change in the legal and regulatory environment, but in a piecemeal way:

- 1999 - Earthquake Athens, Greece: Seismic Design Code, Concrete Technology Code and the Reinforced Concrete Code amended in 1999-2000
- 2001 - Helios Airplane Crash and Wildfire: new framework to embed psychological support for first responders
- 2006 - European Blackout: now code developed to define key technical terms and assign responsibilities
- Various National: Blanket laws banning drones that then get modified emergency response might infringe upon the law in specific crises.

These legal changes, while necessary, point to the possibilities and difficulties of the present system in taking lessons learned an integrating them into a bigger picture. Such challenges make it hard to confirm inclusiveness, distributed justice, and do not create much confidence in any legal frameworks' ability to be resilient, even if responsive.

Inter-agency cross border co-operation within a defined legal framework needs to be implemented on a pre-emptive basis to address international events (2002 - Prestige Oil Spill, Spain; 2010 - Eyjafjallajökull Volcano Eruption). As the law is the formalization of ethics, relying on piecemeal regulatory changes and data sharing in order to manage international events draws the risk of more than just culture-clash, but also bias, injustice, and lack of public understanding, and mission creep.

5.4 Delimiting Liabilities

Pre-emptive codes to assign liabilities could both aid actors involved in the first response and in any subsequent assignation of liability. Complex legal cases to determine liability after an event can damage public trust in all involved (2002 - Prestige Oil Spill, Spain; 2010 - Love Parade Stampede). However, there is a need for accountability in relation to significant failures in duty (2001 - Helios Airplane Crash; 2005 - Buncefield Oil Depot Explosion and Fire). While many regulations are based on tort law to avoid negligence, the actual findings of duties and reasonable standards are often difficult to determine from the laws. Thus, what counts as negligence and what is 'acceptable' or 'enough' are difficult to locate within the legal frameworks.

5.5 Balancing Data Sharing and Privacy

In the light of EU data protection reforms there is a pressing need to clarify the extent to which data can be shared in an emergency situation, as confusion over data sharing agreements can lead to life-threatening delays (2004 - Madrid Train Bombings; 2011 - E.Coli Outbreak, Germany; 2011 - Bombing and Shooting, Norway). Given the focus on international data transfers in the current reform, streamlined measures in relation to emergency situations need to be clarified to facilitate effective responses (2003 - Global SARS Outbreak).

At a wider level there is a need for information to be managed in a way that ensures the communication of key guidance while maintaining privacy. In an age of instant, often crowdsourced, media responses there is a requirement to develop policies to ensure that relatives are informed as a priority while maintaining the privacy of victims (2001 - Helios Airplane Crash and Wildfire). A lack of faith in official information can lead to a reliance of crowdsourced information that can potentially infringe privacy and security (2002 - Prestige Oil Spill, Spain).

Responses of public authorities need to be proportionate to any on-going threat and operate on a time sensitive basis. Once a critical event has passed, authorities need to ensure that they act within the constraints of the regulatory framework which upholds the privacy and human rights of the public (2005 - London Bombings, UK).

5.6 Sharing and Trust

In discussion at the at the SecInCoRe Co-Design Workshop in Manchester in December 2014 (see Appendix 1) an interesting aspect of information sharing became evident: the exchange of information often went well with partners which an organization already worked with but when new groups, agencies or organisations respectively were involved information sharing became more problematic. Besides all ideal pictures of information sharing and all the technical support to do so that were pictured in the prototyping, as one expert put it: "We *can* share, but do we *want* to?" (Emergency Response Expert, SecInCoRe Co-Design Workshop, 2014). There is a misalignment between technological capabilities and political will. These non-technical constraints which limit sharing practices are not only a matter of trust, but also a matter of information politics, especially if the working relationship is new. Even if fire department A knows that B has a special rescue truck, they might not call to inquire about it because they want to get their own truck. They also demonstrate why sharing resources is not enough to make a CIS work.

This was especially the case when it came to volunteers and social media publics, even when they were not actively involved. It became quickly evident that new information sharing technologies, even if not directly designed to engage with the public, are deeply intertwined with fears of impromptu volunteers and commentators, and difficulties of managing them as well as traditional media when faced with unpopular decisions. Even if they would only be sharing with other first responders, the experts present stated how they often decide to hold information back to avoid this potential. However, such decisions to draw barriers become more difficult when politicians see that sharing of information about resources and the resources is technically possible. Trust, then, becomes not a matter of matching data entry with variables of accuracy, but a matter of matching what is technological possible with cultural expectations of social interactions that go even beyond the immediate situation.

5.7 Privatization of Public Goods

Increasingly, public authorities are relying upon private firms to manage public events. Within the private sector, the growth of subcontracting and agency work needs to come with a strict focus on emergency management and the assignation of duties (2001 - Toulouse AZT Explosion). In the light of the scope of human rights protection and its emphasis on the public sphere, there is a need to clarify the liabilities and duties of private companies working in a public capacity because there are different legal (is the contractor company legally bound to serve the public?) and incentive frameworks (are decisions based on public care or private profit?) between private and public organizations (2010 - Love Parade Stampede). Replacing care motives with profit motives also challenges democratic accountability.

5.8 Management and Democratic Participation

The previous literature indicates that disaster response faces a new challenge: how to maintain order and manage the information while responding to the public's response initiatives and request for information, particularly in the face of crowdsourcing. This puts any information technology in a conflicting position of allowing data within to be private and controlled while simultaneously needing to allow mechanism for public engagement without sacrificing the ability to make hard decisions out of the public's critical eye (cp. discussions at December 2014 Co-Design Workshop).

5.9 Balancing Security and Surveillance

Security, in the context of SecInCoRe becomes a much more complicated problem than simply keeping data out of the hands of those who do not have the rights to it. First, the question of who has the rights might change depending on socio-political context. Related to 'Access and Equality', a nuanced awareness of data rights and accessibility is needed in order to avoid exclusion and repression. Second, whose responsibility it is to keep it secure: State? Technology? Citizens? Designers? Responders? (see section 4.2 for a discussion on this in sharing meteorological data across borders). Third, what security is maintained? Is it privacy? Security to share? Security to gather, protest, or democratic expression? Security within the gaps of data? Lastly, as security is managed, it has to balance regulations, trade negotiations (who can have the data and at what expense), and intelligence collection (what would be the benefit of knowing and does that outweigh the risks)? Also, when can security be guaranteed: when entering? While stored? While copied and used?

Security becomes an increasing challenge when dealing with social media and smart cities endeavours. For example, these latter two tools can be used for monitoring urban behaviour of certain users that may have been involved in some "odd" activity to try to determine the intentions of their actions, by combining social media use with their individuals networked 'signature' to determine risk to society. Here, security walks a fine line between surveillance, privacy, consent, pre-emptive risk assessment, and human dignity.

Security should also be transparent, especially when engaging with organizations outside formal response, to increase trust in these interactions.

5.10 Aligning Local Meaning Making

One big issue is the need to create a common concern that is recognizable to all without losing track of the local nuances in practice and sense-making. SecInCoRe is by its nature diverse and thus has at its core a task of creating social cohesion while maintaining diversity. To do so, it should strive to align, not conflate, local meaning making, such as public understanding, criteria for validation and relevance, and tools for determining accuracy. Having these elements aligned, or at least translatable, in ways that the differences are visible and bridgeable is necessary for empathy and trust.

5.11 Designing for Responsibility

> *"It's easy to decide who can access what when all the information is known. When information is being gathered it's less easy" (Emergency Response Expert, SecInCoRe Co-Design Workshop, 2014).*

Questions about transparency, translation, and usefulness made visible that our design decisions do not just enable information sharing, but stretch and challenge informational responsibility. As the experts transposed past disaster response into a future where technologies like SecInCoRe's prototypes were fully functional, two conflicting messages were brought up: 1) the need for "*technology to manage who should know what*" (Emergency Response Expert, SecInCoRe Co-Design Workshop, 2014) and 2) the need for people to learn how to use the technology properly to manage it. To be able to act responsibly, users must be able to make the technology transparent.

But users may also include members of the public who would wish to see a right to data considered in relation to a right to privacy and to what is appropriate for response. Introducing new forms of information sharing affects the tenuous balance between personal liability and the assignment of responsibility. For instance:

> *"We can't fight fires and have everything go back to the public, because it comes back to ethics: if you make the decision to sacrifice someone's property for the greater good and someone puts that out in the public domain, then its going to get back, and then you are suddenly the target of the decision you made" (Emergency Response Expert, SecInCoRe Co-Design Workshop, 2014).*

Or, in another example decisions were made with little knowledge, something that could be misconstrued by a public or hidden by the experts:

> *A: Was it safe to make the hole? No. That's why the town was evacuated.*
>
> *Q: So there was no data about what the container contains?*
>
> *A: Not exact, no.*

While providing information openly can lead to irresponsible use of it by the public, such links can also be vital to responsible use of resources in relation to the public or for the establishment of public trust. Technology needs to enable people to decide about relevance, appropriateness, proportionality, and accuracy.

Technology also needs to enable these decisions over a range of more technical qualities, too. For instance, could a high-resolution still image carry meta-information about how often it is refreshed, the bandwidth needed for sending it? Could the network document how sending this image would affect the overall communication network? Effects of technology use also need to be made transparent in an effort to use technology responsibly.

For example, this conversation took place between two emergency response experts at the SecInCoRe Co-Design Workshop, 2014:

> *R1: If you look at what happened in Schiphol with the air crash, they used TETRA which was designed as an emergency response tool and it failed because of design not technology.*
>
> *R2: No it's not TETRA that failed, it's users that failed, because they are not using it well.*

When it comes to assigning responsibility, and thus blame for failures, the experts made it clear that the questions we need to be asking is: is this really a technology problem or is the reality more to do with obstacles such as parochialism, politics, or governance? This shifting between technology and practice highlights that:

1) Technology alone does not make us smarter;
2) Inclusiveness is not an automatic function of technology, no matter how designed;
3) Joint responsibility needs to be both a design problem and a political one. If not, politics will override any collaboration.

The technological system needs to provide information about the data in such a way that in enables decisions regarding the relevance, usefulness and effects of using that data in this way.

5.12 Striving for Simplicity

Another repeated request from the users was to "make IT simple", yet what 'simple' means was far from clear after the 2014 Co-Design Workshop. The same term was used to mean self-evident, internal workings visible, familiar, every-day, and minimal steps, components or rules. Based on this data, simplicity can mean transparency (as in, it is possible to see the rules of the machine) is integral to trust. It can also mean having the technology be black-boxed – where no questions of it need to be asked; it just works. In these cases, this self-evident nature (i.e., the need to not see the inner-workings) of design is necessary for confidence to be built. In yet other cases it means something aligned with routines and norms that requires minimal learning or change. For this understanding, the focus of design would be on local variations and interpretations of standards. Simplicity, in some combination of all meanings, is needed to spur confidence and trust, even if only part of the whole equation.

5.13 Adaptability

Along similar lines as simplicity, any system needs to be adaptable in order to be both durable and inclusive. This concept derives directly from the literature about standards and classification: if a standard cannot be made locally viable, then it cannot act as a standard because it will not be applicable. If it cannot be made as a standard, it will not last nor will it include everyone that was intended to use it. Moreover, as SecInCoRe's inventory and CIS need to manage taxonomies in the face of dynamism, the system needs to be grounded in some form of adaptability to be able to withstand the constant need for change, exception, and variety as the system learns, expands, and shifts over time. Usefulness is built upon flexibility and reversibility to encourage new solutions from improvised decision-making practices that remain traceable.

5.14 Scalability: managerial, political, situational

Managing information flows in scalable ways should be a central focus of any useful information system, not just managing the production of information from data. The response experts argued that the greater the circle of actors in any information sharing system, the greater the need to delimit accessibility and to guarantee added value for the different roles and responsibilities.

One effect of increasing the range of data sources is a need to create clearer rules for data perimeters. It starts with two questions: How far down the response chain does data need to go? How broad in range does the data need to be? It also involves managing on multiple planes of information sharing at once: sharing between strategic and tactical sections, sharing between agencies or with private companies, sharing in different phases of crisis management, managing public understanding, media messages, and social media trends.

Sharing also needs to be scalable spatially, temporally, and practically so that it can be basic enough to be part of daily practice, durable enough to work on international responses, and adaptable enough to incorporate new practices or technologies as situations call for. To work, SecInCoRe needs to design something, be it a technology or an organisational system, that considers everyday and infrequent incidents, the small and the large, the routine and the exceptional.

5.15 Inclusiveness

Parallel with scalability comes inclusiveness. As SecInCoRe identifies a wide range of data sets to be incorporated into an information space, one aim is to facilitate the inclusion of new, yet vital, data sets and sources. This would bring into view the wider spectrum of people often involved in disaster responses. The idea was welcomed by the response experts at the 2014 Co-Design Workshop, who said we should:

> *'look at how, in effect, information can be drawn from crowdsourcing sources like that, draw information from Twitter… though not an authoritative source, actually say it's there to inform people' (Emergency Response Expert, SecInCoRe Co-Design Workshop, 2014).*

But such enthusiasm came with caveats. Inclusion and accessibility of a wider range of data and sources means greater needs for management. Sharing everything with everyone is both a problem of clogging the communication lines, and of differentiating signal from noise. This invites an ethical question: if you take data from NGOs or the public, do you have to share back? Or, will new generations rely on technology more strongly or will they have more reservations regarding technology operation? Or even, how do you draw on the past while still remaining open to new socio-technical practices that come with each new generations of emergency responders? Bringing in new technologies for information sharing does not automatically mean bringing in more people. Bringing in new technologies places new and old actors in awkward positions of negotiation, where inclusiveness of people, technology, and resources compete with each other in a range of ways.

Along these lines, inclusiveness can also lead to clutter, clogging decision lines instead of providing a higher resolution sense of awareness. New technology to

integrate more information also leads to difficulties with different agencies' capacities in accessing, processing data, and prioritizing the often-conflicting data. More can mean less for some. Rather than collect all, SecInCoRe needs to provide tools that support people in noticing, determining, and improving the quality, including relevance, appropriateness, timeliness, and compatibility of information.

5.16 Translation and Diversity

Bringing together response experts from seven different countries during the 2014 Co-Design Workshop demonstrated how important it is to attend to similarities and differences in:

- Emergency Response Processes and Roles
- Data sets
- Information Systems
- Business Models
- Ethical, Legal and Societal, and Cultural Frameworks for Emergency Service provision
- Languages

But, as one participant stated:

> *'It's not just about sharing the information / data – it also needs to be needed & understood by the recipients' (Emergency Response Expert, SecInCoRe Co-Design Workshop, 2014).*

Even if standardisation progresses, diversity will remain an integral feature in practice, especially when transnational collaboration is needed. Linguistic and conceptual 'translation' is needed to support coordination across different frameworks. But diversity matters even at national levels, where mechanisms such as Local Resilience Forums can be a platform for coordination.

Consequently, a taxonomy should support translation between roles, languages, IT systems, etc. to make a pan-European disaster inventory and a common information space useful. For example, the term 'first responder' does not mean the same thing in all European countries. Nor does the function of an ambulance. A taxonomy that catalogues and makes available these differences to enable one group to understand what is implied by another group's incident report or resource request. Moreover, diverse needs and perspectives shape how data is sought. For instance, when we asked the experts at the Co-Design Workshop to provide examples of data sets they used, this was the resulting list in relation to 'people affected':

Vulnerable people requiring specialist assistance
People whose presence is not compatible with rest-centres
People at risk
People needing evacuation
Number of victims
Survivor/fatality information
People with disabilities
Anyone needing to be rescued?
Anyone still missing?
Location of people at risk

Trapped people?

Instead of translating all these to one data type, the goal of a taxonomy should be to offer a structure that models the differences while helping them talk to each other. A CIS needs to enable the management of different ways of knowing. While before this workshop it was clear that we needed a taxonomy-based system, through the workshop it became clearer that such a system has to support translation in order avoid bias and to maintain autonomy within collaborative interactions. Moreover, joint responsibility can only really exist in a framework that maintains autonomy.

5.17 Transparency

Transparency surfaced first as a crucial issue in the re-enactments of emergency incidents during the 2014 Co-Design Workshop. But transparency can mean two seemingly diametrically opposed things: on the one hand it requires that the inner workings of a technology are visible and clear to users, on the other it means that the user does not need to worry about the complexity of technology's inner workings, because the technology so intuitive it becomes 'invisible' (Weiser, 1991) and can be used unproblematically and without thinking. Both these forms of transparency were highlighted at once when, during the making of prototyping videos at the workshop, one of the experts said: 'What is the CIS? Is that the network or the cloud?*'* The expert's task was to think about how to support more information sharing in a network enabled common information space. It quickly raised questions: What do we mean by a common information space? How would it be used? The emergency response experts had heard all the technical terms before – inventory, common information space, network, infrastructure, cloud – but still struggled to make sense of what these could be used for in practice. The struggles for clear meaning throughout the workshop highlighted the need for transparency to, in part, also derive from translation and diversity in design.

5.18 Making Useful Technology

> *'Are you fighting on the scenario or are you fighting on the technology?*' *(Emergency Response Expert, SecInCoRe Co-Design Workshop, 2014).*

When reliving times of failure in disaster information sharing, the experts did not agree on fault: the user, technology, or context. This made it difficult to decide how technological potential comes to be useful. For instance, one expert brought a printout of a map with superimposed photographs taken from an army helicopter during floods with continued heavy rain, capturing significant infrastructure breakdown. He brought the map, because it had been pivotal for decisions about food distribution and emergency bridge construction, but it had also been difficult to share and make sense of during the response, because the infrastructure for sharing high-resolution images was not directly available and it was not commonly known how to work around this, the end result being literally cutting and pasting with paper and glue. The fault, and thus what would be a useful solution, was not readily assignable. Similarly, another expert stated: 'Increasingly we refer to capabilities rather than equipment or resources.' The conversation kept shifting from one of understanding each system component to discussing overall problems and politics. In other words, to be useful the system itself has to build interactions that manage these politics and capabilities and balance the

right to the data with the most relevant data needed, things that change depending on the situation.

6 Guidelines for human-centred research methodology

In order to follow the principles set out above, non-functional architectural requirements regarding ELSI are described here. These are a collection of meaningful, desirable, consistent and testable qualities that, while non-functional in principle, can and do address aspects of functional behaviour. The formulation of these requirements is ongoing, but is initially derived from:

1. The preliminary inventory of past disaster events (D2.1)
2. Previous literature discussing the ethics of the user-it interactions envisioned (See chapter 2)
3. Lessons from information sharing projects of similar scope (See Chapter 3)
4. Results from a collaborative design workshop
5. Results from a questionnaire about data use practices

Combining these results together this chapter sets out a framework for ELSI that should be considered and incorporated into the design of SecInCoRe. In doing so, first the chapter starts by arguing for a research methodology that best considers these ELSI. It follows this with the description of an early collaborative design workshop designed to elicit ELSI. Drawing on these results as well as the ELSI set out in the previous chapters, this chapter develops ELSI for each aspect of the project, explaining the terminology used, its impact, and suggesting ways of integrating it throughout the design rather than as a test of the design.

By using human-centred research SecInCoRe aims to develop guidelines for methods that involve collaboration between professional experts, social scientists, engineers, and computer scientists that leverage their diverse knowledge, expertise, local practices, and contexts of use. The potential audience for SecInCoRe, and thus users to be included in the design process is wide ranging. Stakeholders include end user, like police authorities and first responders, as well as public users like research, political, standardization organisations, information system provider and even volunteer organisations that are not under government control. Every individual stakeholder could become a user of the system by, for example, requesting information.

Such guidelines are grounded in encouraging a more hands-on understanding of current practices that can simultaneously envision new ways of working. They aim to widen the breath of stewardship to one of joint responsibility in design, so no single social role is placed with the ethical responsibilities regarding the information produced. The guidelines also balance the necessary managerial work of data collection, storage, and exchange with a culture of participation needed to continually curate and maintain an increasingly diverse body of information. Incorporating the social dissolves the false notion of a designer that can foresee all components of a technical system (Dourish, 2001). Pairing these practical engagements with disclosive ethics investigations (Introna, 2007) it becomes possible to uncover unintended consequences that arise as technologies are taken into use. Recording the negotiations that occur between participants can offer insight into the types of translations required by a system of information exchange. These collaborative research methods also need to be able to offer insight into what is feasible

technologically and what needs to be balanced with face-to-face interactions. The methodological guidelines and ELSI rational are described in Table 2.

Table 2 Guidelines for the develop of human-centred research methods

Methodological Guidelines	**Reasons/ELSI Considerations**
Aims for a hands-on understanding of current practices while simultaneously envisioning new ways of working. Users actively working with our ideas to see how they understand them, not just how we understand their ideas	Negotiates multiple understandings rather than rely on one group's understandings of another Leverages diversity in knowledge and expertise Makes visible what needs translation and why, in order to determine how
Incorporates the anticipation of emergent future practices, rather than just focuses on what already is or was done, that can inform both more 'appropriate' and more ambitious innovation.	Develop methods to balance formal vs emergent and local Encourages timeliness of innovation
Covers the full range of stakeholders	To develop a greater awareness and reduction of the power-struggles and injustices perpetuated by the socio-technical system To design to encourage inclusiveness and neutrality Helps maintain individual and community autonomy Distribution of resources Acknowledges the tensions and potentials in public-private partnerships and in government-public/media engagements
Explores the interplay between the social, technological, and organizational. Pay attention to the incidental as well as the immediate	Enables disclosive ethics Helps identify what knowledge is tacit, background, or rule-based and thus in what part of the design process it belongs
Explores various contexts of practice	Broadens view on beneficiaries, usefulness, and necessities

Methodological Guidelines	Reasons/ELSI Considerations
Facilitates practical, not just discursive exploration of futures	Develop awareness of present and foresee potential unintended consequences Incorporates pre-emptive risk management in the design process, rather than just after the fact
Participants become a collective resource for design and produce an environment of mutual learning	Limits biases Balances democratization with local variation and exceptions Distributes expertise, liability, responsibility
Encourages moments of culture-clashes and tension and records the negotiations that occur	First step in developing tools for shared vocabulary and translation of cultures of activity Make visible what is needed to build trust into the system
Study these new technologically augmented practices *in vivo*	Make technologies workings apparent and understandable Makes it possible to see the work of intermediation necessary for translation and recognition of a common object
Provides iterative feedback and ongoing dialogue	Provides versatility and flexibility in structure required for mobility of standards and classifications used Produces a resilient system

For an initial draft of how such methodological guidelines could work as a co-design workshop, please see Appendix 1.

7 ELSI Guidelines for SecInCoRe Design

In this chapter, we set out preliminary ELSI guidelines for SecInCoRe. Given the nested nature of socio-technical innovations within the remit of the project, this is a complex challenge. We begin with a short section that describes the overall SecInCoRe vision and then maps ELSI for each major component/objective of SecInCoRe (As described in D4.1), including barriers to use, opportunities arising, and effects of use, and finally ELSI considerations needed in the design. For each section of SecInCoRe, a separate set of guidelines has been produced since through our research and interactions with disaster response experts it became clear that the different components might have different ELSI challenges. For example, the Inventory needs to deal with issues of categorising links to content, meta-data extraction and making this searchable and accessible, while the Common Information Space (CIS) and Cloud Emergency Information Space (CEIS) need to support collaborative reasoning and information politics as well as lawful data analysis in line with data protection regulation, and Network Enabled Communication (NEC) needs to be secure and scalable, and support trust. When possible it offers suggestions as to paths to pursue to mitigate or address the various ELSI in the design of SecInCoRe. Readers should bear in mind that these considerations are as deeply interconnected as are the different components of the SecInCoRe concept and synthesis and balancing across different demands is necessary. Moreover, this is a first draft of such guidelines, and will be adapted and changed as the project continues.

7.1 The SecInCoRe Concept as a Whole

SecInCoRe works across different scales of innovation, connecting changes in broad moral frameworks with regulatory, technological and social innovation. The aim is to enhance societal security by building a secure dynamic cloud-based concept for information, communication and resource interoperability in multi-agency crisis management, including a common information space. This will be based on a pan-European disaster inventory collating links to information about stakeholders, information systems, resources and data sets, business models, information systems incident command models, and lessons learned, in regional, national as well as cross-European emergencies and disasters.

SecInCoRe starts with a commitment to understand the informational practices people employ to understand risks, to make sense of disasters, to prepare for and to respond to disasters to best address the complex cultural, social, material and political practices that can enable or impede communication and information flows. This understanding is built into how SecInCoRe is envisioned to make a difference. Figure 2 shows a schematic synthesis of the different components.

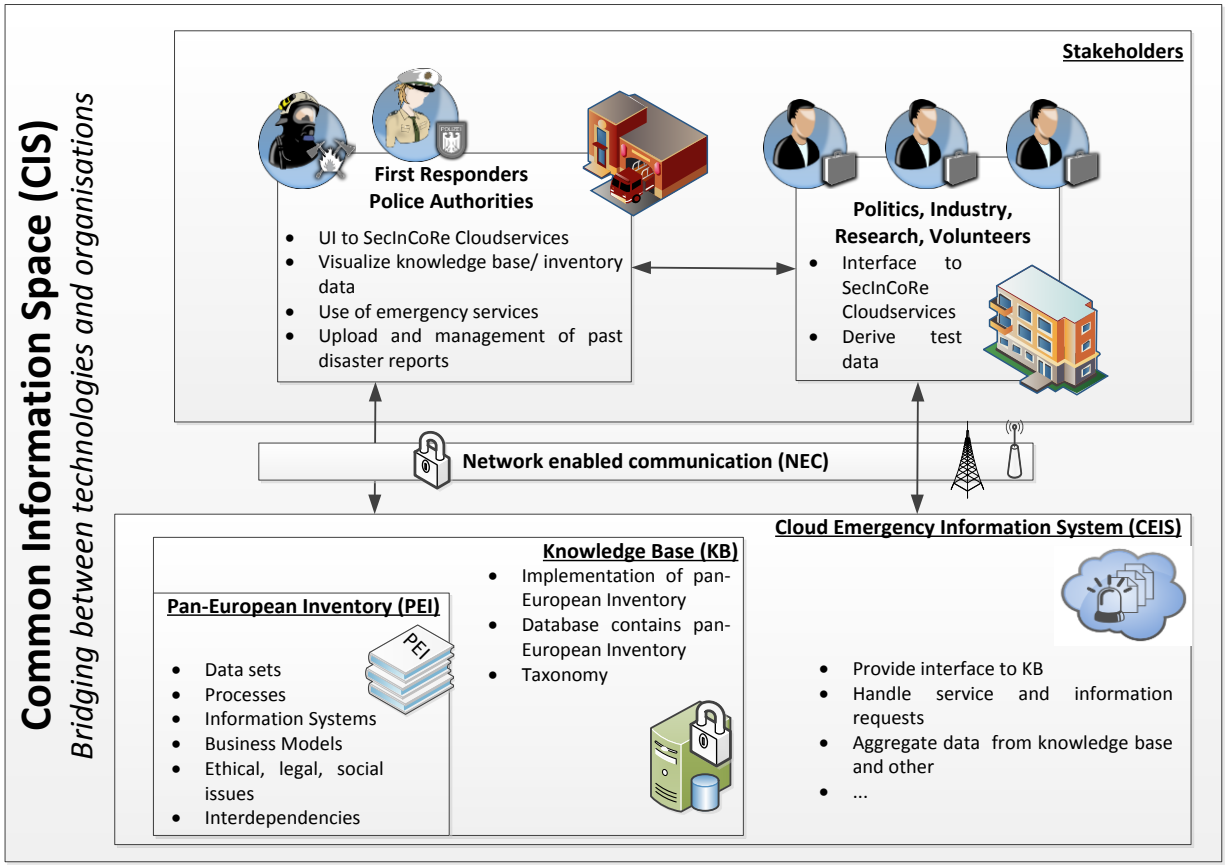

Figure 2. Overview SecInCoRe and its conceptual components (see D4.1 for a detailed description of technical aspects)

Underlying this assembly of technologies and stakeholders and their practices is a broader and more ambitious concept of an 'Internet for disaster related information', complete with a 'Google' search mechanism to dynamically leverage information gathering around a specific disaster. The search would run on meta-information recorded as parties contribute links to disaster relevant information. Key to expanding this 'Internet of disaster related information' concept into a CIS and CEIS is an understanding of and support for the complex informational practices that the multiple stakeholders involved employ in their understanding, management and response to disasters. Powered by this overarching Internet concept, this architecture calls for a set of innovative techniques and mechanisms that can take the idea of a CIS beyond being a mere 'container' or 'ocean' or 'library' of information or a space of resource exchange, towards it being a lived socially produced space for making sense of disasters prospectively, as they unfold and retrospectively. This has two main dimensions:

1) SecInCoRe supports the curation of an immense inventory by tapping into incident management tools and multiple repositories of data, including incident reports, open data, communications data repositories, sensor data and what have you. It supports data curation by highlighting important categories of information, by extracting meta-information and making it searchable, by informing data and incident reporting standards, by supporting via working groups policy changes to obligations for data sharing and incident reporting. It

supports people in entering information by providing incentives (enhanced reputation, collective intelligence) and by providing reassurance that data entered will be treated with respect for the law. When entering data, people will be prompted with ELSI guidelines to consider what level of abstraction or anonymisation the data is at, and what kinds of access restrictions might be needed. Moreover, the structure of data entry and access will also address ELSI in transparent ways (in both sense of the term). Guarantees can be provided that data is secure. And there are translation services that translate between different languages and between different incident command models and processes.

2) SecInCoRe supports social and material human practices of collaboration and sense making, including dialog, interpretation, information politics, modulated disclosure, accountability, simplicity, diversity, multiple perspectives. In designing the CIS it avoids assuming an 'information ideology' that posits that all that is needed to improve societies' capacity to manage and respond to crises is more information, and instead recognises that this is a matter of supporting advanced technologically augmented human reasoning.

The project thus has impact at different scales. It showcases and supports advanced technologically augmented human practices amongst a wide range of stakeholders. It pursues ambitious technological innovation that genuinely understands and supports these practices and does so in a way that is sensitive to ethical, legal, and social opportunities and challenges. It drives policy and regulatory innovation that can realise the most advanced information technology potential. Finally, the project contributes to a critical reflective engagement with the morality of risk and crisis management in information societies facing a century of disasters. By dovetailing these different strands of innovation, the project advances socio-technical innovation that seeks to materialise more secure, desirable, just and morally virtuous futures.

7.2 Concept of an Inventory

The usefulness of a pan-European inventory of disaster information, including past disaster events (D2.1), data sets, command systems including information management processes, information systems and business models (D3.1 & D3.2) and secure dynamic cloud-based common information space concept (D4.1) rests on a basic assumption: that societies can learn from past disasters. However, SecInCoRe needs to approach this from the position that simply having more data does not equal more knowledge. Information does not easily move across organizational and cultural boundaries. The goal of SecInCoRe innovation is to make a system that can support professional practices of information management and information sharing. In this light, the design of an inventory aims to create something more than a database that anyone can access, but a gateway to information that also accommodates and informs a variety of practices, information needs, and command structures. The inventory also aims to be a system to foreground ELSI, issues at the heart of why disaster plans and responses are accepted and trusted by the public being helped. We want it to encourage decision-making that openly acknowledge ELSI. Such ELSI-aware design for public acceptability requires a combination of social, technical, organizational and policy innovation. These different modes of innovation must be synchronised and may

involve everything from intricate detailed ergonomic designs of interfaces to policy change and political pressure.

The aim of the assemblies of technologies brought together in SecInCoRe is to be a gateway to data that are referred to in the inventory rather than a formal repository. It would be impossible and impractical to have it be a repository for all disaster information – the amount of work would be too much and the memory too large. But it can be a gateway to the information stored by emergency agencies and elsewhere – a kind of Internet for disaster information that can be of benefit throughout the entire disaster cycle.

It could provide background information when developing new plans and training/exercises. It could be a resource to consult when faced with a new situation to help formulate new priorities as well as to examine trends in who to involve and ask for help. It could be something referred to when dealing with a new community or a previously un-engaged with socio-economic group to get information about what has worked and has not in those communities or issues that are particularly salient for those groups. It could be used as a research resource, like a library, for disaster reports. Or for new data sets or partners to work with. As a whole, it should act as a community resource, one SecInCoRe initially sets up, where interested community members can contribute and extend it as their use needs. The specific format is still up for question.

7.2.1 Barriers to Use of Inventory

Responsibility for maintenance

Whose job it is to populate and maintain it? It does not fall into the familiar routines already in practice, and thus would require adding new responsibilities to already taxed responders. With this new responsibility comes new liabilities. What if the information is not entered correctly? Or what if the information is missing a security stamp? If it is a community resource and populated by the community, what happens if not everyone is allowed access? Or if only a certain demographic takes on the responsibility of entry, will the information become accidental tools for social injustice in responses designed on basis of the information?

Usefulness

Is it useful during an event, for planning or recovery, for developing lessons learned, to prevent similar situations? How do we balance this use with the need to look at the immediate situation at hand and the time it takes to analyse the information in the inventory? Will it be a management tool for resources and response? Or are the political and legal barriers to such sharing during an event such that offline analysis is what will be useful? Its usefulness is also predicated upon the relationship of the inventory to already existing practices and logics around databases, considering both how databases are the familiarity to and commonly used by our audience.

Data protection

A basic question is what happens to the data that is linked to and shared? Do the rules for security stay the same as it crosses boundaries? Are their exceptions when secure data should be made available? How do we make sure that data is handled in a

secure manner (from entry to various uses)? What parts of data protection are we responsible for?

Managing diversity over time

As the amount of linked data increases, so too does the diversity of data. To be useful, the inventory would need to provide a flexible, ever changing, yet self-evident standard of classification and meta-data to accommodate for the increase in data without abstracting and erasing the diversity.

Managing accuracy

This system would need to be constantly updated and modified by those using it in order to remain valid. These agreements would also have to cover what would be used to determine accuracy? Can it be designed in a way that allows for a diversity of expressions of accuracy, trust, and quality? How can it facilitate the translation between these expressions?

Issues with access

A few different barriers in relation to access and equity emerge, especially considering the range of potential public and private partners, with ephemeral relationships that do not share interests or codes of ethics. What if the inventory is populated with data links that are secure so it does not increase access for sharing? What if someone who needs it does not have physical access to the database? What if someone who can populate it cannot access other data within it? How is equity maintained in all of these cases?

7.2.2 Opportunities when Inventory is used

Pre-emptive risk assessment

Because there is much linked data, it becomes possible to identify trends that would otherwise go unnoticed. These trends can help identify what is truly unique or what might be more symptomatic of a larger socio-political structure. They can also make it possible to see what issues others with similar cases might exist. Necessary frameworks for allocating responsibility and risk communication roles can be developed.

Make more cohesive regulatory changes

While large-scale emergency events precipitate legal and regulatory changes, these changes are often designed to address only the immediate needs as fast as possible. Consequently, the bigger picture is often left unaddressed. While only one use of the inventory, by documenting these changes and their affects on the legal and regulatory environment, then it could become easier to make changes that look beyond the immediate needs and consider the wider issues that led to the immediate situation in ways that make for more sustainable laws.

Building trust and aligning local meaning making

The more connections, examples, cases are drawn upon from regions outside of one's own agency, the greater the trust that can be developed. This is partly because it becomes possible to understand the 'how' and 'why' of decisions that were made, but

it also creates a familiarity between different classification schemas, standards of protocol, terminology, and priorities.

Creating opportunities for greater inclusiveness

Use of the inventory can make visible the range of stakeholders and related resources involved in a disaster response and recovery that might have otherwise been segregated or unknown. This increases the likelihood of more stakeholders being included in some portion of a response for future incidents.

7.2.3 Effects of Use of Inventory

Accountability/Liability

Because they have the data do they then need to respond to it? Or will the person entering the data be held accountable if they did not foresee a risk? Or, what if an effect became only visible in hind-sight, does that mean there are new forms of accountability?

Stifling versatility and adaptability

Because it becomes an archive of linked data and practices, the inventory can potentially stagnate knowledge/encouraging one perspective of expertise. As it is referenced for lessons from similar problems, drawing on those lessons has the potential to recreate the methods instead of innovating or drawing on new tools and practices. While the inventory as a whole envisions a broader set of data within, these issues can appear in different manners depending on when and for what the inventory is engaged with.

Conflating Preparedness, Prevention, and Response

Depending on how it is used, it could conflate different phases of disaster management. According to Lakoff (2008), prevention and preparedness ask for different priorities and standards for communication infrastructures, which in turn can build different relationships between the communities and emergency response organizations. First, prevention focuses on a specific event that might affect the population, bases decisions in risk calculations of past events, and usually requires only a single solution to be prepared for by the authorities. This relationship to disasters is grounded in the assumption that public education and extrapolations from the past can keep a disaster from entering the orderly system. Preparedness, on the other hand, emphasizes mitigation and focuses on protecting the larger infrastructure and building a capacity to manage a range of circumstances. Instead of avoiding catastrophe, demonstrating preparedness approaches disasters as normal occurrences that will inevitably arrive. SecInCoRe's inventory stands at an awkward straddle to these two models: one goal is to learn lessons from specific past disasters to avoid similar situations in the future; the other is to become part of training and exercise regimes to help prepare people for new situations.

Challenge to Expertise

The data and the checklists/structures for input into the inventory can place those traditionally with expertise in positions of defence and rebellion if they feel threatened by the system. It also has the potential to pose a challenge to expertise as locally

formed, instilling standards on all data and removing the local and tacit from the knowledge and stature.

7.2.4 ELSI Guidelines for Inventory

Table 3. ELSI Guidelines for Inventory Design and Use

ELSI Guideline	Potential Pathway Forward
Taxonomy should support translation	We can begin by drawing on other work on this issue, like that of Emergel (http://vocab.ctic.es/emergel/) that has put together a system for translating different uses of the same term to make it easier to merge data sets. Meta-data can become a requirement when imputing anything into the system, that asks for the selection of basic definitions, or at least statement of where the definitions come from so that when it goes through a system like Emergel, it becomes easier to know what needs translation. Focus on reasoning on why categories get accessed (from practices with the data) so that the variations in standards and classification are less important to interoperability. Have an algorithm that can aggregate tags to help develop taxonomy in order to avoid gaps and fragmentation.
Scalable in inclusiveness and function	The inventory should be searchable at many different levels: local, national, regional. It should also be searchable by decision-making need, such that those making strategic decisions can look only at similar situations and scales of action.
Be transparent (inner-workings visible) both linguistically and conceptually, so users can understand, through use, the implications of how they are using it.	As a user is imputing or accessing data, checkboxes should pop up that ask basic questions that reveal how the data within the inventory is organized. When entering data, for example, to determine what level of security:

ELSI Guideline	Potential Pathway Forward
	Does the data contain personal information? ☐ Yes ☐ No If that personal data were redacted, could it be publically accessible? ☐ Yes ☐ No These questions help demonstrate how the data is internally structured as well as what types of security measures are in place. They could also be structured to ask who has used the data, so that other groups could see what kind of data might be useful to them. Map information flow so users can see what they are doing and what others are doing with the data.
Needs to provide tools for analysis of the quality of data (such as determining accuracy, relevance, appropriateness, timeliness).	
Tools for predicting socio-cultural reaction to emergency response	Have a section that is on media coverage of a given response that is searchable by decision type rather than incident type. For example, have it possible to search how the public reacted to having information withheld so that other information priorities could be met (like delaying the information about the reopening of an evacuated region when a newly evacuated area needs the same roads).
Provide mechanisms to delimit and open access to data in a way that	Intimately connected to scalability and transparency, this type of mechanism can

ELSI Guideline	Potential Pathway Forward
offers a nuanced approach	help a user get access to data depending on the situation, not just the type of data (so, in some situations it is acceptable to provide the public or NGOs access to data, while in other cases it is best that access to the inner workings of decision making is limited so that an agency's public authority is not challenged during a response).
Provide data security, in entry, access, and use	For example, make it impossible to copy the data directly, so no copies can be removed from the security system built in to the inventory.

7.3 Concept of an CIS

The SecInCoRe concept of a CIS incorporates the Inventory and a technologically enabled knowledge base and cloud emergency information space (see D4.1 for more explanation of these relationships). The term "Common Information Space" needs to be elaborated in order to better understand how it is a system of relationships rather than simply a common operating picture, shared understanding, a catch-all, or place for resource exchange.

A CIS is a space created by the interactions of diverse stakeholders and stakeholder as they approach a problem from different perspectives, angles, and layers. It does not exist fully form prior to interactions, but is a 'mechanism of interaction' that facilitates translation, negotiation, and sense-making of the objects within by the actors involved (Bannon, L. and Bødker & Bannon, 1997; Bertelsen & Bødker, 2001; Schmidt & Bannon, 1992). The CIS is an emergent socio-technical practice, not a piece of software code that changes form as the interactions, stakeholders, and situation changes.

By providing interpretive context, the CIS supports actors in noticing, determining, and improving the relevance, quality, timeliness, appropriateness, and compatibility of information, in a way that the various groups involved can continually assess and reassess common objectives (Bertelsen & Bødker, 2001; Schmidt & Bannon, 1992). It facilitates expression and communication of alternative perspectives within a common problem domain while also producing boundaries, the combination of which enables trust and translation between communities (Schmidt & Bannon, 1992). Its maintenance also still relies on human mediators and physical spaces (Bertelsen & Bødker, 2001). Vitally, though, a CIS will only work if those involved are mutually dependent on each other's work such that there is an allocation of accountability, which is more than just the need to share each other's resources (Schmidt & Bannon, 1992).

7.3.1 Barriers to CIS

Need for translation

In order to allow for a shared vocabulary and negotiation of vulnerability and appropriate distribution of resources, translation is needed (Rademaekers et al., 2009). Without some common frame of reference and standards for communication, a common object of action (even if local meanings vary) is not possible.

Security

With its flexible structure, it becomes challenging to guarantee security of data, especially if access is in constant flux. Communicating the measures that are in place and constantly making visible the present status and shifts in data access is difficult and can impede trust in the system. There is also the risk that these interactions can be interpreted as violations of personal security via 'secret' monitoring and data sharing in a closed CIS.

Data protection

Data protection becomes even more difficult when issues of consent are involved. Is the situation a state of exception in which consent can be suspended? If so, how does that exception become the norm once the information is shared without consent? Is there a way to prepare the data, meta-data, or links in advance that make these contingent and changing relationship between protection and consent viable?

Clogged lines

If too many people are trying to access the same information or one person is constantly using the entire bandwidth, then the lines of communication will fail and users will lose faith in the system.

Un-Familiarity

A CIS, while it draws on local practices, might ask for users to take on new roles and expectations in times of duress. However, typically at these times people fall back on the familiar and routine.

Trust

Because there are so many sources for data, gathered using a range of techniques and for a range of purposes, knowing what data to trust for a particular situation becomes exponentially challenging and is no longer grounded in local practices and relationships.

Local Variations

One way of approaching the local variations would be the awareness of the respective authorities and their regular update and preparation exercises to accommodate for changes in the local parameters that could influence the effectiveness of the response. Furthermore, such exercises have to be regularly organized from the scale of neighbour prefects and to that of entire nations. Such "drill" routines will assist with the surfacing of potential problems during a real emergency and conclusions reported will assist to refine the procedures in practice.

7.3.2 Opportunities when CIS is used

Inclusiveness

Via the CIS, these different stakeholders all have the potential to interact and/or engage with each other's data and resources in ways that builds reliance. For example, if an emergency call is made, the telecoms company will disclose the caller's location to emergency agencies. Or, a range of NGOs that work closely with the government responders, such as the Red Cross, and commercial organizations, such as insurance companies, supermarkets or hotels, may share information about victims and local resource needs. Or, even if the response is contained to first responders – police, fire, and medical – the different formal structures and languages. Incorporating all the stakeholders can help alleviate an imbalance in data sharing that exists at present: while first responders draw on a range of stakeholders for data, they share data by and large with only other government agencies.

Resilience to information

Because of the flexibility innate to a CIS, it has the potential to produce information and information practices that have greater resilience over time and that can withstand the introduction of new users and new technologies. This would also make any information that populates an inventory less likely to encourage past-patterns as the information itself is derived from malleable relationships.

Increase effectiveness of liaisons

Because of the shared objectives and social cohesion built around a CIS, the liaisons – who are still indispensible – will have greater roles and value to a disaster response.

Joint responsibility

Because the CIS is about interrelationships of necessity rather than individual roles or the sharing of specific resources, working in one spreads the responsibility over all users rather than laying blame or burden on specific actors. Doing so can offer openings for disaster responders to work with less fear of persecution for negligence because it is harder to assign liability. While this is also a potentially negative effect (no risks to decisions) there are also benefits where necessary decisions can get made that might be unpopular but are grounded in the entire network rather than a single organization.

Trust

Because the relationships are built on necessity rather than simply the burden of sharing, then a level of trust has to be negotiated for the CIS to function. As such, in that negotiation, there will be productive work on translation, transparency, and aligning local meaning making.

7.3.3 Effects of Use of CIS

Digital Divides

Because the CIS requires a certain amount of connectivity, there runs the risk of creating digital divides between those that can access the network and those that cannot.

Balancing management and democratic interactions

The CIS has the potential to build into interactions a fine balance required between interactions based in management and more democratic forms of interaction and meaning-making (Jasanoff, 2010). This can help build trust and confidence in the actions of responders act as stewards in society, as well as help build into the responders' decisions and practices an understanding of how the public and other agencies connection actions with the production of vulnerability and resilience. However, one effect of this is an unclear chain of command. Thus, we need to have well defined data sets accessible through the inventory that can guide and assist towards decision making and parameterization. It is equally important that a policy that takes into account the public visibility and accountability for emergency responders is agreed upon based on which actions are directed.

Rights to data

As with any situation where information sharing can be limited, the question arises as to who has the right to access the data and when do they have those rights (for example, does an actors access rights change between planning and response?). These questions will likely be raised throughout any disaster response as some groups are denied entry into the CIS, and other groups are allowed only limited entry. Even on a basic level where a CIS provides only some information for each participant, questions could arise as to what else was there that was not accessible? This can become even more problematic if some of the stakeholders are private entities with data property rights rather than providing only public goods. And, especially if a CIS requires a malleable understanding of data rights, this poses a challenge for the maintenance of privacy.

Social sorting

Also, because a CIS is potentially scalable, in practice some of the stakeholders could be written out of the CIS on a regular basis. Moreover, because the CIS, by nature, has to function on some sort of taxonomy and classification system, these ordering structures also have the potential to sort responders and the public into specific categories of action, privilege, and responsibility in ways that might not work in every locale and context. Also, if one set of values/framing is applied throughout, the system risks perpetuating value creep.

Dehumanized reasoning/formal at expense of informal

As the CIS moves many interactions that might have been face-to-face to a networked realm, it risks dehumanizing reasoning into the rules of programming and system design. It also risks losing the informal aspects of social interaction that make part of a CIS adaptable (Bertelsen & Bødker, 2001).

Adaptability

Being built upon so many perspectives, and being able to change form with the introduction of new stakeholders, new technologies, and new contexts of use, a CEIS offers an adaptable system of information exchange that can grow and evolve with the needs of the situation (and thus be a system of resilience). Such flexibility within standards is required to maintain order over a long term (Jordan & Lynch, 1992; Waugh & Streib, 2006).

7.3.4 ELSI Guidelines for CIS

Table 4. ELSI Guidelines for CIS Design and Use

ELSI Guideline	Potential Pathway Forward
Enable direct communication between users, not just their data	The system needs to work with rather than replace liaisons Have the system pair the virtual interactions with the liaison work
Be built upon a system of necessity, not on the potential for sharing	
Recognizable as common	Needs to make visible different meanings that are involved in ways that make the shared goals the common objects of concern rather than assumptions of the same sense of the situation
Treat interoperability as organizational and emergent rather than technical and rule-based	Have access to data sets/types not be predetermined but decided in situ. Have those decisions be joint (so one user cannot impeded access to another without the other's consent).
Balance democratic interactions and inclusiveness with clear chains of commands	
Be disclosive (in terms of ethics, technology, etc.)	
Safeguard against social sorting	Make visible and trackable as the CEIS is functioning who is included, who has requested access, who has been excluded. Include forms for asking questions and gathering information about why access is granted or denied.
Consider various institutional perspectives and public understanding to building empathy, trust, confidence in decisions	

7.4 Concept of a Network Infrastructure

The Network Infrastructure should work independently from used devices or operating systems. The overall goal is to develop an intelligent solution for mobile network evaluation to decide when to use which network and how to combine them to enhance Quality of Service (QoS). That means the user does not have to care about the

communication infrastructure and how he is connected to. The visionary case includes a user operating his device with multi-enabled technology that selects and connects to the best network in range. The definition of best is depending on the QoS of the user. Further the user can be added to the secure TETRA/TETRAPOL network by scanning a key from an authorized rescue organization. To enhance the coverage and capacity of networks at incidents scenes wireless mesh networks are used to connect places without network coverage (e.g., indoor scenes) with command post and the Internet to enable CIS access.

7.4.1 Barriers to Use of Network Infrastructure

Maintaining security

Insure that collected data is only used on the client's device and not transmitted to third parties in a way that creates confidence in the technology and users. Along these lines, a certain amount of prediction is required of user behaviour, something that is difficult in situations of duress.

Access

While access has already been discussed in the previous section, in relation to the more technical aspects, actors are faced with access problems due to missing credentials for WiFi, availability caused by coverage problems, or even locations with no coverage at all.

Managing data with the need for democratic participation

When dealing with multiple perspectives and goals, it becomes a challenge to define a Quality of Service that does not imposing values from one agency/region onto another.

Validity of data and simulations

Considering the data is generated at the scene of a disaster, it is difficult to create simulations that will offer the range of potential use-cases. As a result, simulations produced to test the network as well as to train and test the practices engaging with the network could be set up in ways that excludes some users and uses, impeding the ability for the system to become part of a routine.

Simplicity/Familiarity

If it does not fit into the routines already in practice, it will be harder to deploy.

Automation

If much of this work is done automatically, then transparency becomes a problem. Moreover, automation can pose a challenge when dealing with unforeseen situations of use or users, as well as pose a challenge for the adaptability necessary for system resilience.

7.4.2 Opportunities when Network Infrastructure is used

Interpersonal communication in networked space

Because the network architecture acts as a basis for information exchange in NLOS (non-line of sight) scenes, it also makes it possible to increase the personal

interactions in the system, replicating aspects of face-to-face interactions, as well as encouraging interoperability between individuals and organisations.

Trust

Any situation has a range of knowledge at play required for the establishment of trust, but most specifically there are three forms: tacit, background, and rule-based. It is relatively easy to design into a technology rules, but much harder to incorporate the tacit and general background information. The network architecture brings in some of the aspects of the tacit (can see the responders in action at the scene) and background (can get some pictures of the scene) that inform the interpretation of and engagement with the rule-based technology making possible more effective, collaborative, and shared decision-making.

Access

A new form of access potentially emerges, as those who would otherwise be unable to access the scene now have access to it. Doing so can provide a greater number of people with a localized situational awareness that would otherwise not be possible, making more effective decision-making.

7.4.3 Effects of Use of Network Infrastructure

Clogged lines

Have to make sure that use patterns and practices do not clog the lines of communication, either impeding the use of this data or making this data the only data that gets used. Support is needed for ‘configuring awareness’ not just in relation to other people, but also between people and agencies, systems, infrastructures. People should be able to use lines creatively, in an improvised manner (as is always the case in disaster response), but they should be able to do so with consideration for others’ needs. The blindness to the clogging effects was at the heart of the TETRA ‘misuse’ described in chapter 5.

Secrecy

The way in which data gets shared within the CIS runs the risk of becoming a form of secret surveillance as it balances data sharing with privacy and consent issues, as the aggregated data discloses more than its parts.

Gap-filling

This system of gathering information directly from the scene has more than just technological value. When there are data gaps during an incident, the procedure is to collect data at the scene of the incident to then be distributed to those in need. In doing so, it can help provide context for the rest of the data gathered about an incident.

Social sorting and fragmentation

Because of the innate security built into the system, as well as the ability to choose the network with whom information is shared, there is the risk that groups will be fragmented and sorted into generic categories of access, rights, and responsibilities rather than dealt with as the situation demands.

Adaptability and Scalability

Because the system is designed around on-demand capacity, it has scalability of various types built into it.

Normalization of Surveillance

As recording scene and sharing that data live become part of routine response, privacy and surveillance issues emerge, and thus security. While the system might create greater efficiency in response, it also increases visibility of scene without consent and without the ability to maintain privacy or anonymity.

Privacy

The system needs to gather personal data to work. What personal data can is use for identifying the user needs? Velocity, gps tracks, history of application? What are the implications of such gathering and sharing? How will consent be managed?

7.4.4 ELSI Guidelines for Network Infrastructure

Table 5. ELSI Guidelines for Network Infrastructure Design and Use

ELSI Guideline	Potential Pathway Forward
Privacy issues need to be directly addressed in self-evident ways	By installing the application/program the user has to accept that personal data is collected for optimizing the network connectivity. Pair the technology with practices around data storage and sharing that manage the privacy and security of those caught in the line of sight.
Networking needs to clearly display access to avoid the pitfalls of fragmentation.	When choosing those to invite in the network, have the system automatically inquire about related agencies based on previous records (e.g. cases form inventory)

ELSI Guideline	Potential Pathway Forward
	You've requested that Fire join into your response network to this flood. Other similar incident responses have also included these agencies. Please check on them to include as well. ☐ Environmental Agencies ☐ Consulting Security ☐ Local Police ☐ Red Cross ☐ Governmental GIS agencies Please click on an agency to find out what kind of data they used and why they were granted access.
Security needs to balance the right to privacy, data sharing, and access	
Data gathered from the scene and shared within this infrastructure has to be treated with the same respect as that without public consent to manage the incidental data capture.	Right to access has to be balanced with the right to be forgotten. This has to be done for a variety of data types, including: • real-time • asynchronous • pictures • video • text or other static information
Ensure that the user agreed on data collection for quality derivation.	
Has to be flexible enough to manage a range of seeming opposites	Centralized vs decentralized interactions: client to server (centralized storage and distribution of data) vs peer 2 peer (decentralized storage and distribution of data). usability on different end user devices (one user – many devices) Different presentation needs and capacities

8 Appendix 1: Description of initial methods/co-design workshop

A first draft of a co-design methodology was implemented at a workshop with users on 9-10 December 2014. Participants included with 13 emergency response experts from a range of backgrounds and 12 interdisciplinary members from SecInCoRe. The objectives of the workshop were to learn about past disaster events and current practice, to learn about technological potential and its relation to practice, and to co-design early visions of our socio-technical project. The overarching goal was to experiment with new ways of working that integrate new technologies. More immediate aims were to learn more about problems in information sharing, to gather variations in interpretations of data, validity, usefulness, and accuracy, to understand how technological capabilities affect decisions and practice, and to chart ethical, legal, social opportunities and challenges. We documented the results via video, audio, and hand written notes (Figure 3).

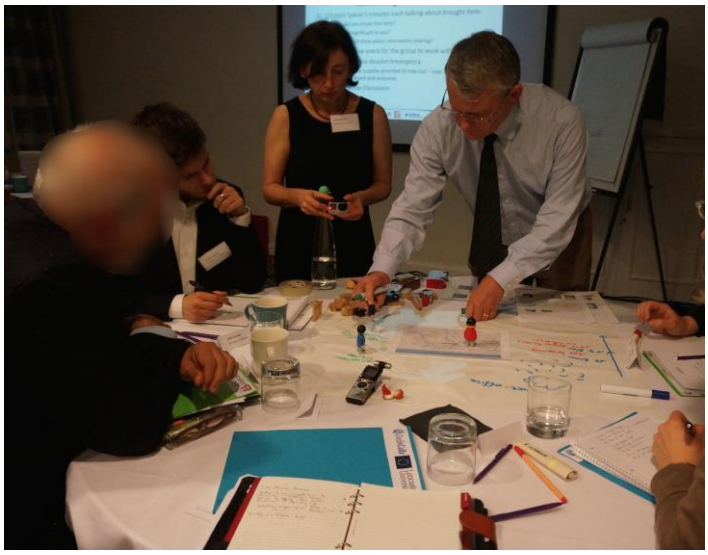

Figure 3. Documenting the workshop and co-designed practices.

The workshop methods were designed around disaster re-enactments (past and future) in small groups. To ground these re-enactments in concrete experiences, each expert was asked to bring an object that was representative to them of a significant moment regarding interoperability during a disaster. As some of the key moments were re-enacted, focusing on crisis response efforts, particular emphasis was made on demonstrating practices and difficulties in information sharing and making sense of information. Then, after being introduced to our present design ideas and prototypes, we asked them to revisit their re-enacted scenarios and appropriate all of these prototypes. The experts were invited to re-enact the cases as if they already had these technologies and to make three-five minute video prototypes (Mackay & Fayard, 1999) that demonstrated how technology and new ways of working could come together fruitfully. Within and between activities was much time for open discussion. The activities, design results, and aimed for elicited ELSI are listed in Table 6.

Table 6. Methodology Schema

Collaborative Activity	Design Result	ELSI Aim
Discussion of representative objects in small groups	Describe present practices	Understanding of current situation into which any innovation would be inserted. Understanding of local variations of conceptions of relevance, security, liability, and responsibility.
Re-enactment of disaster scene in small groups	Via the observation of socio-technological practices. Identify present problems, including commonalities and areas of difference between experts. Diagrams of spatial-temporal interactions needed for response success.	Develop a picture of planning and response needs as well as ELSI that exist at present. Grasp how they negotiate tensions and tools they use to translate and align local meaning making or recognize activities as common.
Presentation of our design conception plus large-group discussion	List of questions and debates about the value of the design	Identify how users understand our design and how that understanding diverges from ours to better understand their value structures and practices.
Making prototype videos in small groups	Discussions of what the new technologies can/should do. Videos of how the experts understand what our design does and how that relates to what they already do.	Identify new solutions and new ways of posing problems previously not envisioned. Develop an understanding of what is needed for social cohesion, confidence, and trust. Gather issues of concern and barriers to practice as emerged from these engagements.

Split into small groups, each expert began by presenting specific instances, via objects they brought, of emergency response in which issues interoperability stood out (Figure 4). Each group picked a past disaster event and re-enacted key moments of the crisis response efforts, with a particular emphasis on demonstrating practices and difficulties in information sharing and making sense of information (Figure 5). We followed the re-enactments with a presentation of SecInCoRe's design ideas, utilising protoypes (Figure 6). Our presentation was placed at this point in order to elicit more directed responses and imaginings from the experts at the scene, while also allowing them to structure their interactions based on their previous experiences.

Figure 4. Pivotal information captured in photographs taken from army helicopter.

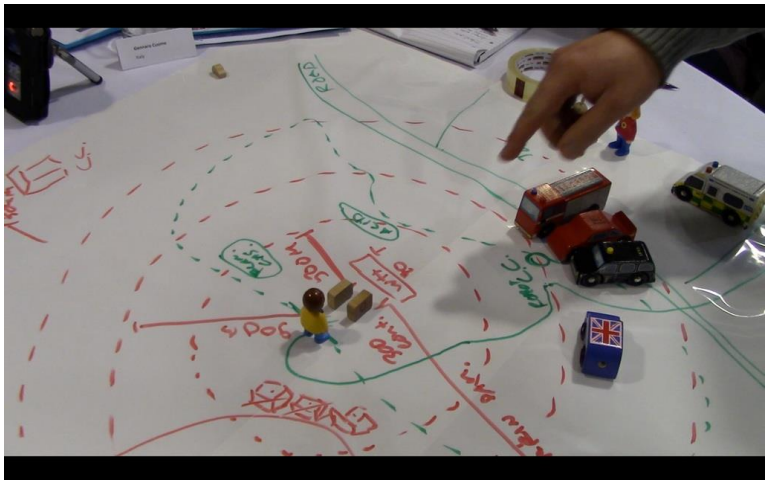

Figure 5. The moment where it was decided to allow workers from a factory affected by radioactive dust spillage to leave without recording their details.

Figure 6. The equipment used to demonstrate the imagined networking infrastructure

What we ended up getting was a range of questions that were less technical and more ontological as they worked to understand our basic categories and relations between them. The idea of a place, be it an inventory or a common information space, for all information to go was neither novel nor standardisable, and thus led to a great deal of confusion. The emergency response experts questioned the basic categories of design that we had been working under, revealing how potential users would understood (or not understood) these concepts as well as encouraging us to revisit our own goals for the project.

The day ended with a quick round of brainstorming data types, sources, and reasons for gathering. The activity was low-tech, asking each expert to write on large sticky-notes as many items as they could for each section. Then we assembled them together, first having each put up what they designated as different, then grouping the remaining items together. The aim of the activity was three-fold: 1) to encourage the experts to think about the different types of data they need to consider for the disaster re-enactments; 2) to create a very rough draft of European-wide data needs; and 3) to draw out the nuanced differences in those data needs (Figure 7). While the goals were ambitious (and not fully achieved), this type of activity also demonstrated that while there was much overlap in how the data was used, the users were not completely clear as to the details of the data that were required for decision-making. In many cases, they were unaware of where the data came from, or what technical format it arrived in. From this we as designers can learn both how our users engage with the data, what responsibility they have in relation to it, and the limitations of their responses to our questions about data in particular.

Figure 7. Photograph of the sticky notes collected for the data types

Appropriating these design ideas and data lists, the experts then re-enacted their cases as if they had our technology and made three to five minute video prototypes (Mackay and Fayard, 1999) of socio-technical innovation that demonstrated how technology and new ways of working could come together fruitfully (Figure 8). Discussions happened between each event as each group demonstrated their results to each other and we discussed the results as a large group.

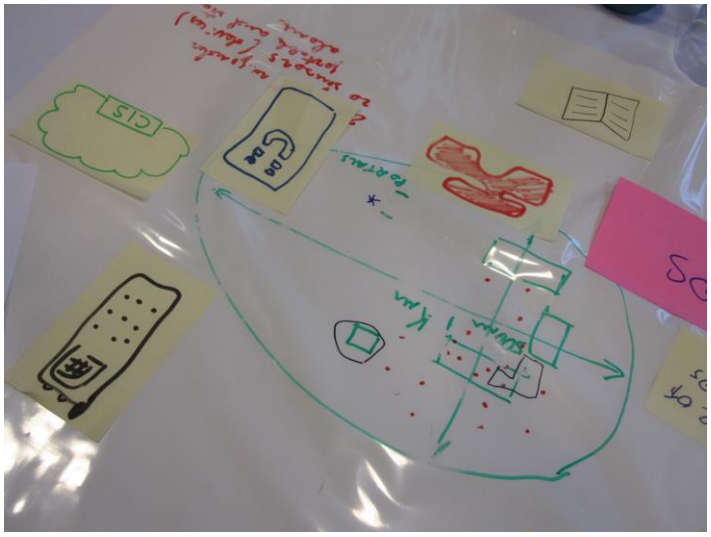

Figure 8. The experts revisiting their mapped out case study as if they were using our technology, explaining when and how the technology would (or wouldn't) get incorporated.

We found that in this process we were jointly making sense of the different components of the innovation envisaged in the project. We also found that we were not simply 'collecting' 'user perspectives', but were forced to rethink our own conceptions of the goals, potentials and constraints involved. A discussion on ELSI illustrates this most colourfully, as ethical, legal and social complexities became visible that neither group had foreseen, challenging notions of diversity, usefulness, responsibility, trust, traceability, and autonomy.

9 References

Alexander, D. E. (2013). Social Media in Disaster Risk Reduction and Crisis Management. *Science and Engineering Ethics*, 1–17. http://doi.org/10.1007/s11948-013-9502-z

Allen, D. K., Karanasios, S., & Norman, A. (2013). Information sharing and interoperability: the case of major incident management. *European Journal of Information Systems*. http://doi.org/10.1057/ejis.2013.8

Baker, K. S., & Bowker, G. C. (2007). Information ecology: open system environment for data, memories, and knowing. *Journal of Intelligent Information Systems*, *29*(1), 127–144. Retrieved from http://connection.ebscohost.com/c/articles/26147317/information-ecology-open-system-environment-data-memories-knowing

Bannon, L. and Bødker, S., & Bannon, L. and B. S. (1997). Constructing Common Information Spaces. In *ECSCW*. Retrieved from http://www.ul.ie/~idc/library/papersreports/LiamBannon/ECSCW.htm

Bellotti, V., Back, M., Edwards, W. K., Grinter, R. E., Henderson, A., & Lopes, C. (2002). Making sense of sensing systems. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems Changing Our World Changing Ourselves CHI 02*, 415. Retrieved from http://portal.acm.org/citation.cfm?doid=503376.503450

Bertelsen, O. W., & Bødker, S. (2001). Cooperation in massively distributed information spaces. In *ECSCW01 Proceedings of the seventh conference on European Conference on Computer Supported Cooperative Work* (pp. 1–17). Kluwer Academic Publishers. Retrieved from http://portal.acm.org/citation.cfm?id=1241868

Boin, A., & Ekengren, M. (2009). Preparing for the World Risk Society: Towards a New Security Paradigm for the European Union. *Journal of Contingencies and Crisis Management*, *17*(4), 285–294. http://doi.org/10.1111/j.1468-5973.2009.00583.x

Boulden, J. (2004). International crisis response and a Canadian role. *International Journal*, *59*(4), 801–813.

Bowker, G., & Star, S. L. (2000). *Sorting Things Out: Classification and Its Consequences*. Cambridge, Massachusetts: MIT Press.

Brändström, A., Bynander, F., & Hart, P. 't. (2004). Governing by Looking Back: Historical Analogies and Crisis Management. *Public Administration*, *82*(1), 191–210. http://doi.org/10.1111/j.0033-3298.2004.00390.x

Buck, D. A., Trainor, J. E., & Aguirre, B. E. (2006). A Critical Evaluation of the Incident Command System and NIMS. *Journal Of Homeland Security And Emergency*

Management, *3*(3), 1–27. Retrieved from http://www.bepress.com/jhsem/vol3/iss3/1

Büscher, M., Liegl, M., Perng, S., & Wood, L. (2014). How to follow the information? A Study of informational mobilities in crises. *Sociologica*, *1*. http://doi.org/10.2383/77044

Büscher, M., Liegl, M., Rizza, C., & Watson, H. (2015). ELSI in Crises: Doing IT More Carefully. *International Journal of Information Systems for Crisis Response and Management.*, *(forthcomi*.

Büscher, M., Liegl, M., & Wahlgren, P. (2014). *Ethical, Legal and Social Issues: Current Practices in Multi Agency Emergency Collaboration: Deliverable 12.2, BRIDGE Project.* Retrieved from http://www.bridgeproject.eu/downloads/d12.2_bridge_elsi.pdf

Buscher, M., Perng, S., & Wood, L. (2013). Privacy, Security, Liberty: Informing the Design of EMIS. In T. Comes, F. Fiedrich, S. Fortier, J. Geldermann, & L. Yang (Eds.), *Proceedings of the 10th International ISCRAM Conference – Baden-Baden, Germany, May 2013*. Retrieved from http://eprints.lancs.ac.uk/62141/1/ELSI_FP_Privacy_pre_final.pdf

Büscher, M., Perng, S.-Y., & Liegl, M. (2015). Privacy, Security, Liberty: ICT in Crises. *International Journal of Information Systems for Crisis Response and Management (IJISCRAM)*, *(forthcomi*.

Büscher, M., Simonsen, J., Bærenholdt, J. O., & Scheuer, J. D. (2010). *Design research. Synergies from interdisciplinary perspectives.* (J. O. . B. M. . D. S. J. . S. J. Bærenholdt, Ed.). Routledge. Retrieved from http://www.amazon.com/Design-Research-Interdisciplinary-Perspectives-ebook/dp/B0042FZZ0O

Callon, M., & Muniesa, F. (2005). Peripheral Vision: Economic Markets as Calculative Collective Devices. *Organization Studies*, *26*(8), 1229–1250. http://doi.org/10.1177/0170840605056393

Cavoukian, A. (2001). Taking Care of Business: Privacy by Design. Toronto. Retrieved from http://www.ontla.on.ca/library/repository/mon/2000/10296375.pdf

Cavoukian, A. (2012). Privacy and Drones : Unmanned Aerial Vehicles, (August), 1–27.

Chesbrough, H. W. (2003). *Open Innovation: The New Imperative for Creating and Profiting from Technology* (p. 227). Harvard Business Press. Retrieved from http://books.google.com/books?hl=en&lr=&id=4hTRWStFhVgC&pgis=1

Coady, C. A. J. (2004). Terrorism, Morality, and Supreme Emergency. *Ethics*, *114*(4), 772–789. http://doi.org/10.1086/383440

Crowther, K. G. (2014). Understanding and Overcoming Information Sharing Failures : Journal of Homeland Security and Emergency Management. *Journal of Homeland Security*, *11*(1), 131–154. Retrieved from http://www.degruyter.com/view/j/jhsem.2014.11.issue-1/jhsem-2013-0055/jhsem-2013-0055.xml

De Laet, M., & Mol, A. (2000). The Zimbabwe Bush Pump: Mechanics of a Fluid Technology. *Social Studies of Science*, *30*(2), 225–263. http://doi.org/10.1177/030631200030002002

Dougherty, C. (2008). While the Government Fiddled Around, the Big Easy Drowned: How the Posse Comitatus Act Became the Government's Alibi for the Hurricane Katrina Disaster. *Northern Illinois University Law Review*, *29*, 117–47.

Dourish, P. (2001). *Where the action is*. *Where the Action is*. {M}{I}{T} {P}ress.

Dratwa, J. (Ed.). (2014). *Ethics of Security and Surveillance Technologies* (Opinion no, pp. 1–165). Brussels: European Group on Ethics in Science and New Technologies to the European Commission.

Dyzenhaus, D. (2006). Schmitt v. Dicey: Are States of Emergency Inside or Outside the Legal Order? *Cardozo Law Review*, *27*, 2005–2039.

Edwards, P. (2010). *A Vast Machine*. Cambridge, MA: MIT Press.

Egan, M. J. (2011). The Normative Dimensions of Institutional Stewardship: High Reliability, Institutional Constancy, Public Trust and Confidence. *Journal of Contingencies and Crisis Management*, *19*(1), 51–58. http://doi.org/10.1111/j.1468-5973.2010.00632.x

Ehn, P. (2008). Participation in design things, 92–101. Retrieved from http://dl.acm.org/citation.cfm?id=1795234.1795248

ENISA. (2012). *Emergency Communications Stocktaking. A study into Emergency Communications Procedures*. Retrieved from http://www.enisa.europa.eu/media/news-items/report-looks-at-improving-emergency-communications

eScience. (2012). Earth faces a century of disasters, report warns. Retrieved November 4, 2012, from http://esciencenews.com/sources/the.guardian.science/2012/04/26/earth.faces.a.century.disasters.report.warns

European Commission. (2013). *Risk-Benefit Analyses and Ethical Issues: A guidance document for researchers complying with requests from the European Commission Ethics Reviews*. Luxembourg: Publications Office of the European Union.

European Commission. (2014). *Factsheet: Rules under Horizon 2020*. Retrieved from http://ec.europa.eu/research/horizon2020/pdf/press/fact_sheet_on_rules_under_horizon_2020.pdf

Federal Coordinator for Meteorological Services and Supporting Research. (1998). *Report on the Implementation of the Interdepartmental Meteorological Data Exchange Systems (IMDES)* (pp. FCM–R12–1998). Washington D.C.

Feenberg, A. (2010). Ten Paradoxes of Technology. *Techné*, *14*(1), 3–15. http://doi.org/10.5840/techne20101412

Ferejohn, J., & Pasquino, P. (2004). The law of the exception: A typology of emergency powers. *International Journal of Constitutional Law* , *2* (2), 210–239. http://doi.org/10.1093/icon/2.2.210

Fiore-Silfvast, B., & Neff, G. (2013). What we talk about when we talk data: Valences and the social performance of multiple metrics in digital health. *Ethnographic Praxis in Industry Conference Proceedings*, *2013*(1), 74–87. http://doi.org/DOI: 10.1111/j.1559-8918.2013.00007.x

Fortun, K. (2001). *Advocacy after Bhopal: Environmentalism, Disaster, New Global Orders*. Chicago: University of Chicago Press.

Franco, Z., Flower, M., Whittle, J., & Sandy, M. (2015). Professional Ethics and Virtue Ethics in Community-Engaged Healthcare Training. In D. E. Mitchell & R. R. K. (Eds.), *Professional Responsibility: Advances in Medical Education* (pp. 211–229).

Frickel, S. (2008). On Missing New Orleans: Lost Knowledge and Knowledge Gaps in an Urban Hazardscape. *Environmental History*, *13*(4), 643–650.

Fritzsche, P. (2005). The Archive and the Case of the German Nation. In A. Burton (Ed.), *Archive Stories*. Durham, NC: Duke University Press.

Gao, H., Barbier, G., & Goolsby, R. (2011). Harnessing the crowdsourcing power of social media for disaster relief. *IEEE Intelligent Systems*, *26*, 10–14. http://doi.org/10.1109/MIS.2011.52

Godschalk, D. R. (2003). Urban Hazard Mitigation: Creating Resilient Cities. *Natural Hazards Review*, *4*, 136–143. http://doi.org/10.1061/(ASCE)1527-6988(2003)4:3(136)

Goodspeed, R. (2014). Smart cities: moving beyond urban cybernetics to tackle wicked problems. *Cambridge Journal of Regions, Economy and Society* . http://doi.org/10.1093/cjres/rsu013

Graham, G. (2014). Too-smart cities? Why these visions of utopia need an urgent reality check. *The Guardian, 13 March*.

Graham, S., & Thrift, N. J. (2007). Out of order: understanding repair and maintenance, *24*(3), 1–25. http://doi.org/10.1177/0263276407075954

Green, S. (2007). Looting, Law, and Lawlessness. *Tulane Law Review*, *81*, 1129–1174.

Greenfield, A. (2013). *Against the smart city*. Do projects; 1.3 edition. Retrieved from http://www.amazon.co.uk/Against-smart-city-The-here-ebook/dp/B00FHQ5DBS

Harrald, J. R. (2006). Agility and Discipline: Critical Success Factors for Disaster Response. *The ANNALS of the American Academy of Political and Social Science*, *604*(1), 256–272. http://doi.org/10.1177/0002716205285404

Hartswood, M., Procter, R., Slack, R., Voß, A., Buscher, M., Rouncefield, M., & Rouchy, P. (2008). Co-realization: toward a principled synthesis of ethnomethodology and participatory design. *Resources CoEvolution and Artifacts*, *14*(2), 59–94. Retrieved from http://www.springerlink.com/index/q710532862167p41.pdf

Haythornthwaite, C., Lunsford, K. J., Bowker, G. C., & Bruce, B. C. (2006). Challenges for research and practice in distributed, interdisciplinary collaboration. *New Infrastructures for Knowledge Production: Understanding E-Science*, 143–166.

Hertzum, M., & Simonsen, J. (2011). Effects-Driven IT Development: Specifying, realizing, and assessing usage effect. *Scandinavian Journal of Information Systems*, *23*(1). Retrieved from http://aisel.aisnet.org/sjis/vol23/iss1/1

HM Government. (2013). *Emergency Response and Recovery Non statutory guidance accompanying the Civil Contingencies Act 2004*. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/253488/Emergency_Response_and_Recovery_5th_edition_October_2013.pdf

Hoffman, S., & Oliver-Smith, A. (2002). *Catastrophe & culture: The anthropology of disaster*. *School of American Research advanced seminar series* (p. xii, 312 p.). Santa Fe, NM: School of American Research Press; J. Currey.

Hollands, R. G. (2008). Will the real smart city please stand up? *City*, *12*(3), 303–320.

Humanitarian OpenStreetMap. (n.d.). Mongolia, mapping Ulaanbaatar. Retrieved from http://hot.openstreetmap.org/projects/mongolia_mapping_ulaanbaatar

Hutchins, E. (1995). *Cognition in the Wild*. Cambridge, MA: MIT Press.

Ignatieff, M. (2005). The Ethics of Emergency. In (pp.). Edinburgh: Edinburgh University Press. In *The Lesser Evil* (pp. 25–53). Edinburgh: Edinburgh University Press.

International Committee of the Red Cross. (2013). *Professional standards for Protection Work* (pp. 1–115). Retrieved from http://www.icrc.org/eng/assets/files/other/icrc-002-0999.pdf

Introna, L. D. (2007). Maintaining the reversibility of foldings: making the ethics (politics) of information technology visible. *Ethics and Information Technology*, *9*(1), 11–25. Retrieved from http://eprints.lancs.ac.uk/4729/

Jarman, A., Sproats, K., & Kouzmin, A. (2000). Crisis Management: Toward a New Informational "Localism" in Local Government Reform. *International Review of Public Administration, Let*, *5*(2), 81–97. Retrieved from http://scholar.google.co.uk/scholar?hl=en&q="Crisis+management:+Toward+a+new+informational"&btnG=&as_sdt=1,5&as_sdtp=#0

Jasanoff, S. (2010). Beyond calculation: A Democratic Response to Risk. In A. Lakoff (Ed.), *Disaster and the politics of intervention* (pp. 14–40). Columbia University Press.

Jennings, B., & Arras, J. (2008). *Ethical Guidance for Public Health Emergency Preparedness and Response: Highlighting Ethics and Values in a Vital Public Health Service* (pp. 1–192). Retrieved from http://www.cdc.gov/od/science/integrity/phethics/docs/White_Paper_Final_for_Website_2012_4_6_12_final_for_web_508_compliant.pdf

Jillson, I. (2010). Protecting the public, addressing individual rights. Ethical issues in Emergency Management Information Systems for Public Health Emergencies. In B. van de Walle, M. Turoff, & S. Hiltz (Eds.), *Information systems for emergency management.* (pp. 46–61). New York: Sharpe.

Jordan, K., & Lynch, M. (1992). The Sociology of a Genetic Engineering Technique: Ritual and Rationality in the Performance of the "Plasmid Prep." In J. Fujimura & A. Clarke (Eds.), *The Right Tools for the Job* (pp. 77–114). Princeton: Princeton University Press.

Kendra, J., Wachtendorf, T., & Quarantelli, E. L. (2003). The evacuation of lower Manhattan by water transport on September 11: an unplanned "success". *Joint Commission Journal On Quality And Safety*, *29*(6), 316–318.

Kenk, V. S., Križaj, J., Štruc, V., & Dobrišek, S. (2013). Smart Surveillance Technologies in Border Control. *European Journal of Law and Technology*, *4*(2). Retrieved from http://ejlt.org/article/view/230/378/

Kitchin, R. (2013). The real-time city? Big data and smart urbanism. *GeoJournal*, *79*(1), 1–14. http://doi.org/10.1007/s10708-013-9516-8

Lakoff, A. (2007). Preparing for the next emergency. *Public Culture*, *19*(2), 247. Retrieved from http://anthropos-lab.net/wp/publications/2007/01/lakoff_prepare.pdf

Lakoff, A. (2008). The generic biothreat, or, how we became unprepared. *CULTURAL ANTHROPOLOGY*, *23*(3), 342–399. http://doi.org/10.1525/can.2008.23.3.399

Langheinrich, M. (2001). Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems, 273–291. Retrieved from http://dl.acm.org/citation.cfm?id=647987.741336

Larkin, G. (2010). Unwitting partners in death-the ethics of teamwork in disaster management. *The Virtual Mentor : VM*, *12*(6), 495–501. http://doi.org/10.1001/virtualmentor.2010.12.6.oped1-1006

Latonero, M., & Shklovski, I. (2011). Emergency Management, Twitter, and Social Media Evangelism. *International Journal of Information Systems for Crisis Response and Management*, *3*(4), 1–16. Retrieved from http://www.igi-global.com/article/emergency-management-twitter-social-media/60612

Latour, B. (1992). Where are the Missing Masses? Sociology of a Few Mundane Artefacts. In W. E. Bijker & J. Law (Eds.), *Shaping Technology, Building Society: Studies in Sociotechnical Change* (pp. 225–258). Cambridge, Mass.: MIT Press.

Lave, J. (1988). *Cognition in Practice: Mind, Mathematics and Culture in Everyday Life*. Cambirdge: Cambridge University Press.

Liegl, M., Büscher, M., & Oliphant, R. (2015). Ethically Aware IT Design for Emergency Response: From Co-Design to ELSI Co-Design. In *Proceedings of the ISCRAM 2015 Conference* (p. (forthcoming)). Kristiansand, Norway, 24-27 May 2015.

Liu, S. (2014). Crisis Crowdsourcing Framework: Designing Strategic Configurations of Crowdsourcing for the Emergency Management Domain. *Computer Supported Cooperative Work (CSCW)*, 389–443. http://doi.org/10.1007/s10606-014-9204-3

Liu, S., & Palen, L. (2010). The New Cartographers: Crisis Map Mashups and the Emergence of Neogeographic Practice. *Cartography and Geographic Information Science*, *37*(1), 69–90.

Mackay, W., & Fayard, A. (1999). Video brainstorming and prototyping: techniques for participatory design. *CHI'99*, (May), 118–119. http://doi.org/10.1145/632716.632790

Mahony, M., & Hulme, M. (2012). Model migrations: Mobility and boundary crossings in regional climate prediction. *Transactions of the Institute of British Geographers*, *37*, 197–211. http://doi.org/10.1111/j.1475-5661.2011.00473.x

Maurer, S. M., Firestone, R. B., & Scriver, C. R. (2000). Science's neglected legacy. *Nature*, *405*(6783), 117–120. Retrieved from http://dx.doi.org/10.1038/35012169

Meier, P. (2012). Improving Beijing's urban transportation with crowdsourced mapping. Retrieved from http://www.ushahidi.com/2012/06/05/ushahidi-beijing/

Mendonça, D., Jefferson, T., & Harrald, J. (2007). Emergent Interoperability: Collaborative Adhocracies and Mix and Match Technologies in Emergency Management. *Communications of the ACM*, *50*(3), 44.

Merz, M. (2006). Embedding Digital Infrastructure in Epistemic Culture. In C. Hine (Ed.), *New infrastructures for knowledge production: Understanding e-science* (pp. 99–119). London: Idea Group Inc.

Motorola. (2012). *the Future of Integrated Command and Control Starts Now*.

Moynihan, D. P. (2009). The Network Governance of Crisis Response: Case Studies of Incident Command Systems. *Journal of Public Administration Research and Theory*, *19*(4), 895–915. Retrieved from http://jpart.oxfordjournals.org/cgi/content/abstract/19/4/895

Muhren, W. J., & Van de Walle, B. (2010). Sense-making and information management in emergency response. *Bulletin of the American Society for Information Science and Technology*, *36*(5), 30–33.

Mullagh, L., Blair, L., & Dunn, N. (2014). Beyond the smart city: Reflecting human values in the urban environment. In L. Patrono & W. Leister (Eds.), *roceedings from SMART 2014, The Third International Conference on Smart Systems, Devices and Technologies SMART 2014* (pp. 43–46). Paris: IARIA.

Murphy, T., & Whitty, N. (2009). Is human rights prepared? Risk, rights and public health emergencies. *Medical Law Review*, *17*, 219–244. http://doi.org/10.1093/medlaw/fwp007

Nam, T., & Pardo, T. A. (2011). Conceptualizing smart city with dimensions of technology, people, and institutions. *Proceedings of the 12th Annual International Conference on Digital Government Research*, 282–291.

Nelson, C. B., Steckler, B. D., & Stamberger, J. A. (2011). The evolution of hastily formed networks for disaster response: technologies, case studies, and future trends. In *… (GHTC), 2011 IEEE* (pp. 467–475). Seattle, WA: IEEE. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6103680

Norris, C. (2002). From personal to digital: CCTV, the panopticon, and the technological mediation of suspicion and social control. In D. Lyon (Ed.), *Surveillance as Social Sorting* (pp. 249–281). Routledge.

Office of the Federal Coordinator for Meteorological Services and Supporting Research. (2010). *National Plan for Disaster Impact Assessments: Weather and Water Data* (pp. FCM–P33–2010). Washington, DC.

Palen, L., Hiltz, S. R., & Liu, S. B. (2007). Online forums supporting grassroots participation in emergency preparedness and response. *Communications of the ACM*, *50*(3), 54–58. http://doi.org/10.1145/1226736.1226766

Pauwels, E. (2007). Ethics for researchers. Brussels: European Commission.

Perrow, C. (1984). *Normal Accidents: Living with High-Risk Technologies*. Princeton, NJ: Princeton University Press.

Petersen, K. (2014). Producing space, tracing authority: mapping the 2007 San Diego wildfires. *The Sociological Review*, *62*, 91–113. http://doi.org/10.1111/1467-954X.12125

Prieur, M. (2009). *Ethical Principles on Disaster Risk Reduction and People's Resilience*. Retrieved from http://www.coe.int/t/dg4/majorhazards/ressources/pub/Ethical-Principles-Publication_EN.pdf

Quarantelli, E. L. (1994). *Looting and Anti-Social Behaviour in Disasters. Preliminary Paper #205* (pp. 1–5). Retrieved from http://dspace.udel.edu/bitstream/handle/19716/590/PP205.pdf?sequence=1

Rademaekers, K., Eichler, L., Holt Andersen, B., Madsen, N., & Rattinger, M. (2009). *Strengthening the EU capacity to respond to disasters: Identification of the gaps in the capacity of the Community Civil Protection Mechanism to provide assistance in major disasters and options to fill the gaps – A scenario-based approach* (p. 213). Rotterdam. Retrieved from http://ec.europa.eu/echo/civil_protection/civil/prote/pdfdocs/Final Report - scenario study.pdf

Rake, E., & Njå, O. (2009). Perceptions and performances of experienced incident commanders. *Journal of Risk Research*, *12*(5), 665–685. Retrieved from http://www.informaworld.com/openurl?genre=article&doi=10.1080/13669870802604281&magic=crossref

Ramirez, L., Buscher, M., & Wood, L. (2012). *Domain Analysis - Interoperability and Integration. Bridge project Deliverable D2.2*.

Randalls, S. (2010). Weather profits: Weather derivatives and the commercialization of meteorology. *Social Studies of Science* , *40* (5), 705–730. http://doi.org/10.1177/0306312710378448

Rizza, C., Pereira, Â. G., & Cuervo, P. (2013). Do-it-yourself Justice-Considerations of Social Media use in a Crisis Situation: The Case of the 2011 Vancouver Riots. In *Proceedings of the 10th International ISCRAM Conference – Baden-Baden, Germany, May 2013* (pp. 411–415).

Rogerson, S. (2009). Landscapes of ethical issues of emerging ICT applications in Europe. *Communication*. Retrieved from http://hdl.handle.net/2086/2475

Sandin, P., & Wester, M. (2009). The moral black hole. *Ethical Theory and Moral Practice*, *12*(3), 291–301. http://doi.org/10.1007/sl0677-009-9152-z

Scheppele, K. L. (2006). North American Emergencies: The Use of Emergency Powers in Canada and the United States. *International Journal of Constitutional Law*, *4*, 213–43.

Scheuerman, W. E. (2006). Survey Article: Emergency Powers and the Rule of Law After 9/11*. *Journal of Political Philosophy*, *14*(1), 61–84. http://doi.org/10.1111/j.1467-9760.2006.00256.x

Schmidt, K., & Bannon, L. J. (1992). Taking CSCW seriously. *Computer Supported Cooperative Work*, *1*(1), 7–40. http://doi.org/10.1007/BF00752449

Schmitt, C. (2012). Definition of Sovereignty. In A. M. Viens & M. J. Selgelid (Eds.), *Emergency Ethics* (The Librar, pp. 3–15). Farnham, UK: Ashgate Publishing, Ltd.

Sekula, A. (1986). The Body and the Archive. *October*, *39*, 3–64. http://doi.org/10.2307/778312

Shanley, L., Burns, R., Bastian, Z., & Robson, E. (2013). *Tweeting up a Storm. The Promise and Perils of Crisis Mapping*. Retrieved from http://www.wilsoncenter.org/sites/default/files/October_Highlight_865-879.pdf

Smith, S. M. (2004). *Photography on the Color Line*. Durham, NC: Duke University Press.

Sorell, T. (2003). Morality and Emergency. *Proceedings of the Aristotelian Society*, *103*(1), 21–37. http://doi.org/10.1111/j.0066-7372.2003.00062.x

St. Denis, L. A., Hughes, A. L., & Palen, L. (2012). Trial by Fire: The Deployment of Trusted Digital Volunteers in the 2011 Shadow Lake Fire. In *Proceedings of the 9th International ISCRAM Conference – Vancouver, Canada, April 2012* (pp. 1–10). Retrieved from http://www.cs.colorado.edu/users/palen/Home/Articles_by_Year_files/TrustedDigitalVolunteersStDenisHughesPalen.pdf

Stallings, R. A., & Quarantelli, E. L. (1985). Emergent Citizen Groups and Emergency Management. *Public Administration Review*, *45*, 93–100 CR – Copyright © 1985 American Societ. http://doi.org/10.2307/3135003

Star, S. L., & Griesemer, J. R. (1989). Institutional ecology,translations' and boundary objects: Amateurs and professionals in Berkeley's Museum of Vertebrate Zoology, 1907-39. *Social Studies of Science*, *19*(3), 387. Retrieved from http://sss.sagepub.com/content/19/3/387.short

Starbird, K. (2011). Digital Volunteerism During Disaster : Crowdsourcing Information Processing. *Search*.

Starbird, K. (2012). What "Crowdsourcing" Obscures: Exposing the Dynamics of Connected Crowd Work During Disaster. *Ci2012*, 8. http://doi.org/arXiv:1204.3342

Starbird, K., Maddock, J., Orand, M., & Achterman, P. (2014). Rumors, False Flags, and Digital Vigilantes: Misinformation on Twitter after the 2013 Boston Marathon Bombing. In *iConference 2014*. Retrieved from http://faculty.washington.edu/kstarbi/Starbird_iConference2014-final.pdf

Starbird, K., Palen, L., Hughes, A. L., & Vieweg, S. (2010). Chatter on the red: what hazards threat reveals about the social life of microblogged information. *Proceedings of the 2010 ACM Conference on Computer Supported Cooperative Work*. Savannah, Georgia, USA: ACM. http://doi.org/10.1145/1718918.1718965

Steinberg, T. (2000). *Acts of God: The Unnatural History of Natural Disaster in America*. New York: Oxford University Press.

Suchman, L. (2007). *Human-Machine Reconfigurations* (p. 314). Cambridge University Press. Retrieved from http://books.google.com/books?id=VwKMDV-Gv1MC

Tapia, A. H., & LaLone, N. (2015). Crowdsourcing Investigations: Crowd Participation in Identifying the Bomb and Bomber from the Boston Marathon Bombing. *International Journal of Information Systems for Crisis Response and Management (IJISCRAM)*, *(forthcomi*.

Törpel, B., Voss, A., Hartswood, M., & Procter, R. (2009). Participatory Design: Issues and Approaches in Dynamic Constellations of Use, Design and Research. In A. Voss, M. Hartswood, R. Procter, M. Rouncefield, R. S. Slack, & M. Buscher (Eds.), *Configuring User-Designer Relations*. London: Spring-Verlag.

Townsend, A. (2013). *Smart Cities: Big data, civic hackers, and the quest for a new utopia*. London: W.W Norton and Company Inc.

Turoff, M., Chumer, M., Van De Walle, B., & Yao, X. (2004). The design of a dynamic emergency response management information system (DERMIS). *Journal of Information Technology*, *5*(4), 1–35.

United Kingdom Department for Business Innovation and Skills. (2013). *BIS research paper no. 135. Global innovators: International case studies on smart cities*. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/249397/bis-13-1216-global-innovators-international-smart-cities.pdf

Urry, J. (2007). *Mobilities* (p. 336). Polity.

Vaughan, D. (1996). *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA*. Chicago: University of Chicago Press.

Von Schomberg, R. (2007). *From the ethics of technology towards an ethics of knowledge policy & knowledge assessment*. *Economy and Society*.

Wallis, J. C., Rolando, E., & Borgman, C. L. (2013). If We Share Data, Will Anyone Use Them? Data Sharing and Reuse in the Long Tail of Science and Technology. *PLoS ONE*, *8*(7). http://doi.org/10.1371/journal.pone.0067332

Walsh, J. P. (2010). From Border Control to Border Care: The Political and Ethical Potential of Surveillance. *Surveillance & Society*, *8*(2), 113–130.

Walzer, M. (2006). *Arguing About War*. *Notes* (p. 224). New Haven: Yale University Press. Retrieved from http://opac.rero.ch/get_bib_record.cgi?db=ne&rero_id=R003707879

Washburn, D., Sindhu, U., Balaouras, S., Dines, R. A., Hayes, N. M., & Nelson, L. E. (2010). *Helping CIOs Understand "Smart City" Initiatives: Defining the Smart City, Its Drivers, and the Role of the CIO*. Cambridge, MA: Forrester Research, Inc.

Watson, H., & Finn, R. L. (2013). Privacy and ethical implications of the use of social media during a volcanic eruption : some initial thoughts. In *Proceedings of the 10th International ISCRAM Conference – Baden-Baden, Germany, May 2013* (pp. 416–420).

Waugh, W. L., & Streib, G. (2006). Collaboration and Leadership for Effective Emergency Management. *Public Administration Review*, *66*(s1), 131–140. Retrieved from http://doi.wiley.com/10.1111/j.1540-6210.2006.00673.x

Weiser, M. (1991). The Computer for the Twenty-First Century. *Scientific American*, *265*(3), 107–114. Retrieved from http://www.springerlink.com/index/u4428p7158361143.pdf

Weitzner, D. J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., & Sussman, G. J. (2008). Information accountability. *Communications of the ACM*, *51*(6), 82–87. Retrieved from http://dl.acm.org/ft_gateway.cfm?id=1349043&type=html

Wertsch, J. (1998). *Mind as Action*. New York: Oxford University Press.

White, H. (1978). The Fictions of Factual Representation. In *Tropics of Discourse: Essays in Cultural Criticism* (pp. 121–134). Baltimore, MD: JHU Press.

Woolgar, S. (1990). Configuring the user: the case of usability trials. *A Sociology of Monsters Essays on Power Technology and Domination*, *38*(S1), 58–99.

Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2013). A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges. *Communications Surveys & Tutorials, IEEE*. http://doi.org/10.1109/SURV.2012.021312.00034

Yang, D., Zhang, D., Frank, K., Robertson, P., Jennings, E., Roddy, M., & Lichtenstern, M. (2014). Providing real-time assistance in disaster relief by

leveraging crowdsourcing power. *Personal and Ubiquitous Computing*, 1–10. http://doi.org/10.1007/s00779-014-0758-3

Zack, N. (2009). *Ethics for Disaster* (Vol. 2010, p. 143). Lanham, Md.: Rowman & Littlefield Publishers. Retrieved from http://books.google.com/books?hl=en&lr=&id=JjBOYQHYVh0C&pgis=1

Zilgalvis, P. (2009). Ethics and Governance in the 7th framework programme (pp. 1–14). Retrieved from http://ec.europa.eu/research/conferences/2009/rtd-2009/presentations/ethics/p_zilgalvis___ethics_and_governance_in_the_7th_framework_programme.pdf

Zuckerman, I. (2006). One Law for War and Peace? Judicial Review and Emergency Powers between the Norm and the Exception - Zuckerman - 2006 - Constellations - Wiley Online Library, *13*(4). Retrieved from http://0-onlinelibrary.wiley.com.fama.us.es/doi/10.1111/j.1467-8675.2006.00416.x/full