GUEST EDITORIAL PREFACE

Special Issue on How to do IT more Carefully: Ethical, Legal, and Social Issues (ELSI) in IT Supported Crisis Response and Management

Monika Büscher, Centre for Mobilities Research, Mobilities.lab, Department of Sociology, Lancaster University, Lancaster, UK

Michael Liegl, Centre for Mobilities Research, Mobilities.lab, Department of Sociology, Lancaster University, Lancaster, UK

Caroline Rizza, Economics, Management and Social Sciences Department, Telecom ParisTech, Paris, France

Hayley Watson, Trilateral Research and Consulting, London, UK

INTRODUCTION

It seems clear that 'technology that provides the right information, at the right time, and in the right place has the potential to reduce disaster impacts' (Koua, MacEachren, Turtun, Pezanowski, Tomaszewski, & Frazier, 2010:255). In a century of disasters (eScience, 2012) where nothing is so certain as that another crisis is around the corner and emergency response services are under intense pressure to produce more efficient, collaborative and effective responses and plans, investment in information technology (IT) is often seen as pivotal. Enquiries into the implications of ever deeper integration of IT into emergency response and management for humanity, justice, liberty, and the social contract between societies and emergency responders may seem a burden, but design that is sensitive to ethical, legal and social issues (ELSI) is also recognised as critical to leveraging the potential of new technologies. If emergency services are to utilise (and to control media operated) Remotely Piloted Aerial Systems (RPAS), for example, if they should engage the public with the help of social media, or share information between different agencies and information systems in line with data protection laws, technologies must support

awareness of ELSI and practices of addressing them. This is a complex challenge.

Repeated, sometimes spectacular failures of IT projects highlight the transformative momentum inherent in IT innovation and raise questions about the straightforward usefulness of technology (Ellebrecht and Kaufman, this issue). Worldwide, up to 85% of IT projects fail, at an estimated cost of over $6.2 trillion (Sessions, 2009), and crisis management has a long history of such failures. In two prominent examples of major technology investment – the London Ambulance System in 1992, and more recently the UK FiReControl project, the systems failed because they did not support, indeed incapacitated the local practices of responders. They were abandoned, wasting millions of pounds (Shapiro, 2005; Committee of Public Accounts, 2011). The failure of such systems has ethical, legal and social causes and implications that go far beyond the financial aspects. Indeed, some analysts argue that 'the belief that more data or information automatically leads to better decisions is probably one of the most unfortunate mistakes of the information society (Hollnagel & Woods 2005: 7). It is important to recognise that technology cannot 'provide' the right information at the right time, in the right place, but people can. People gather, sort, visualise, analyse, reason about, and reason with information, they assess its accuracy, relevance, quality, they share or withhold it, they can make sense of it, or not, they may discount it, or draw others' attention to information in ways that communicates their judgement about its relevance, quality or import. Technology can greatly enhance these practices, but it can also undermine, obstruct, or transform them.

Increased reliance on technology can make emergency response and management more dependent on fragile network and data infrastructures, make the work more complex and error-prone and it can engender far-reaching transformations of the emergency services and society. For example, emergency situations can call for exceptions to fundamental and constitutional rights. At a recent symposium, European security experts debated the importance of ELSI research for innovation in Border Surveillance and Search and Rescue[1], calling for the law to catch up with technological innovation, so that, for example, restrictions on the interconnection of information systems for CCTV, face recognition and databases of known convictions for hooliganism could be lifted in France. Yet many European states, especially countries like Romania or Germany, who have experienced totalitarian regimes, are suspicious of such suspension of normal legal and moral rules and values, often fuelled (but not always warranted) by fear of a breakdown of public moral order in emergencies (Barnard-Wills 2013). Their unease is due to the experience that such exceptions can erode important civil liberties, and the fact that 'the wrong kind' of IT innovation in crisis management can amplify a detrimental 'securitization' of society (Aradau & Munster, 2011, Büscher, Perng & Liegl, this issue).

Against this backdrop, some fundamental ethical questions arise for emergency response practitioners, politicians, policy makers, citizens, non-citizens (such as tourists, legal and illegal immigrants), designers and researchers: How can IT design and implementation be done more effectively, more mindful of transformative effects and wider societal implications? How can it be done more benignly? Concerns over IT project failures, the insufficiency of 'more information' for good decisions, and the effects of creeping securitization on civil liberties may suggest 'Don't do IT' as an answer for some. However, the increase in the frequency and severity of disasters in the 21st century of disasters, involving increasingly urbanized and ageing populations is also a massively powerful engine for IT innovation in crisis management. Indeed, it seems that the IT juggernaut into emergency response is unstoppable. Moreover, IT can uniquely enhance risk analysis, communication and collaboration. Thus 'Do IT more carefully' would be a better maxim. But how can this be achieved?

To clarify what 'more careful' might mean, there is a need to better understand ethical, legal and social issues relating to IT supported

emergency response. With this special issue, we contribute six papers to shape more proactive and integrated ELSI-aware design approaches. In this introductory overview, we begin by providing a short review of the socio-political context. This is followed by a discussion of the positively and negatively disruptive nature of IT innovation in crisis response and management, and specifically the role of 'unintended consequences'. The individual papers that follow focus on considerations related to IT innovation and use in crisis management and response in different contexts, ranging from IT support for triage in mass casualty incidents (Ellebrecht and Kaufmann) to restrictions placed on use of mobile devices in organisations (Ford, Stephens & Ford), to the use of social media and the Internet during the 2010 Eyjafjallajokull volcano eruption (Watson & Finn), the 2011 Vancouver riots (Rizza, Guimarães Pereira & Curvelo), and the 2013 Boston Marathon bombing (Tapia & LaLone). The special issue concludes with a discussion of the relationship between privacy, security and liberty in the context of efforts to support emergent interoperability between multiple information systems and stakeholders in 'smart city' contexts (Büscher et al.). We briefly summarise key insights these papers allow.

By exploring diverse impacts on the organisation of emergency response and the people involved, these papers build on contributions from the Information Systems for Crisis Response and Management (ISCRAM) community, where a long-standing commitment to explore ethical and social aspects of innovation in crisis response and management exists. The papers have been developed from contributions to special tracks on Ethical, Legal and Social Issues (ELSI) at ISCRAM conferences in 2013 and 2014. The individual papers illuminate several different, important dimensions of ELSI and we summarise them here to chart core themes. A key insight is that while ethical, legal, and social issues are a matter of material, socio-technical practices and the ways in which people use technology, it is critical to acknowledge – carefully and creatively – that technology itself is not neutral. It actively enacts and shapes morality. A 'disclosive' approach to ethical, legal and social issues can reveal emergent ethical implications – which may pose both challenges and opportunities. By providing a summary of a study that illustrates this in an exemplary way, we prepare for a conclusion that calls for more careful IT innovation in crisis response and management. Here, we delineate what future work is needed to translate the long-standing commitment within ISCRAM to understand ethical, legal and social aspects of innovation into critical, constructive and creative debates about what might constitute 'better' IT supported crisis response and management, and how ELSI research can inform 'better' design and use of technologies.

ELSI AND THE INFORMATIONALIZATION OF CRISIS RESPONSE

Technology has always played an important role in the laws, ethics and social and material practices of emergency response. Physical technology such as breathing apparatus for fire-fighters, fire engines and fire fighting technologies, portable defibrillators for medical personnel, guns and body armour for police have augmented the capabilities of emergency responders for many decades. Policy tools, such as incident command systems, too, have shaped the nature of response (Buck, Trainor, & Aguirre, 2006; Moynihan, 2009). What or who can be rescued or protected changes, as do the processes and practices involved, and therewith the ethics and politics of emergency response. IT introduce another dimension of augmentation.

There has been an 'informationalization' of crisis response and management, following in the footsteps of similar developments in other industries and services. The term refers to an ever more intimate integration of ever more information into economic processes and practices with the help of information technology, starting with the just-in-time logistics for materials and goods in post-fordist economies (Lash &

Urry, 1994), and leading into contemporary forms of 'knowing capitalism' and 'Lifeworld. Inc' (Thrift 2005, 2011), where pervasive collection and processing of data about people's everyday interactions and complex actuarial, 'qualculative' analytics allow corporations ever greater prediction, agility and control. In emergency response, informationalization can support enhanced risk assessment, preventative measures and learning from past events, as well as increased surge capacity, data sharing, communication and collaboration between emergency responders, closer engagement with people affected by disasters and mobilization of 'collective intelligence'. But informationalizing socio-economic processes can also engender far-reaching transformations of these processes. In the domain of crisis management, the use of digital radio in over 125 countries in the world[2] and the rise of social media (Palen, Vieweg, Sutton & Liu 2009; Letouzé, Meier, & Vinck 2013) have fundamentally changed emergency communications practices, for example. Furthermore, when data can be shared more easily and to greater effect, exceptions from data protection regulations may foster surveillance and social sorting and erode values of freedom and democracy. The recent scandal over NSA surveillance starkly highlights the challenges to informational self-determination and privacy arising in the context of IT use in security policy and practice. The ways in which IT are designed and appropriated are deeply entangled with how societies conceive of risks, respond to crises, and facilitate freedom. The informationalization of emergency response is a form of 'disruptive innovation', that is, innovation that transforms the social, economic, political, and organizational practices that shape this domain (Chesbrough, 2003).

Yet, even a recently edited comprehensive compendium of research in emergency ethics, law and policy (Campbell, 2012) pays little attention to technology, and IT ethics in crisis management is somewhat of a new field of study. One of the first publications to tackle the challenge explicitly is Jillson's chapter 'Protecting the Public, Addressing Individual Rights' in Van de Walle, Turoff and Hiltz' *Information Systems for Emergency Management* (2010). She 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 can complicate adherence to core ethical principles of non-maleficence and beneficence, respect for human dignity, and distributive justice (equal access).

In their current use of IT, emergency responders often air on the side of caution when faced with ethical, legal or social uncertainties, such as doubt about informational boundaries in multi-agency collaboration. They often choose not to share data. Fragmentation of response through 'silo-thinking' is a common result and a challenge to ethical conduct (Cole, 2010). Paradoxically, this is, at least partially, a result of the very capability of information systems to support data sharing. ELSI research shows that the reasons raise complex questions about accountability, responsibility and the social contract between society and emergency service professionals and volunteers. The social contract idea stipulates that society grants emergency responders a range of benefits in return for their commitment to save others even in the face of personal risk. Such benefits include 'perhaps most importantly, a great degree of professional autonomy' and the provision of adequate training and tools (Jennings & Arras, 2008:110). Digital logs provide new opportunities to learn from experience in post-disaster reviews of response efforts, but they also allow new ways of holding professionals to account (Bech Gjørv, 2012; Cartlidge, 2012), transforming ideas of professional autonomy. In an environment where IT enable ever more detailed post-disaster expert reviews of disaster response efforts based on extensive records of professional communications and decisions, such data can be treated as evidence for malpractice in a way that lacks appreciation of the real time context of these communications and decisions. It may

attract blame and punishment and as a result, professionals may become uncertain about their reluctant to express themselves freely and clearly or take risky decisions.

(Un-) Intended Consequences

Technology can engender such unintended consequences for ethical, lawful and socially responsible and effective conduct, ranging from impacts on professional integrity and judgement to a securitization or militarization of everyday life. Before we delve into concrete detail through a review of the contributions to this special issue and an example from the wider literature, it is useful to examine the concept of 'unintended consequences'.

The notion of 'unintended consequences' features prominently in the literature on risk, especially on risk assessment of technology (Beck, 1992; Merton, 1936), but it is unclear whether such consequences are considered avoidable or inescapable, whether they are known, unknown or unknowable in advance. Furthermore, what precaution could be taken to avoid or mitigate them? Is this something that can be done before a technology gets implemented or need there be an ongoing monitoring process, for detecting and managing such consequences:

For and by whom were these consequences unintended? Does 'unintended' mean that the original intent was not achieved, or that things happened outside the scope of that imagined intent? The notion also carries an implied exoneration from blame, since anything 'unintended' was implicitly unforeseeable, even if things somehow subsequently went awry. [...] The narrative of unintended consequences sets aside the possibility of acting irresponsibly on inadequate knowledge ... (Wynne & Felt, 2007, p. 97).

For designers and practitioners engaged in IT innovation in emergency response and management this statement implies a need to take responsibility for unintended consequences, by trying to notice, anticipate and know them, to amplify positive effects and to mitigate or avoid negative ones. If we examine the 10 core ethical principles of emergency response as defined by the International Federation of Red Cross and Red Crescent Societies Code of Conduct and their translation into components of emergency services in relation to practices and virtues needed to accomplish them, we formulate some examples of how capacities to perform such services, practices and virtues are transformed in interaction with IT (Table 1). A complex pattern of sometimes contradictory intended and unintended effects becomes visible. For example, compassion, charity, hope, empathy, resilience, respect and effective communication can be supported through technologies that allow more immediate and richer communication, and mapping and visualization of vulnerable populations, needs and available resources. As such, IT can help provide services that alleviate suffering faster and more generally support enactment of ethical principles of humanity. At the same time, such technologies could increase information overload and overwhelm responders' capacities to compile information in a meaningful way. Similarly, the tireless, unbiased application of computational logic could be used to support impartiality through fair and equal distribution of resources, but it can also allow forms of identifying vulnerable or risky populations and techniques for social sorting that undermine values of impartiality (Table 1).

Many of the ambiguities listed here are explored in depth in the individual contributions to this special issue. They show that core ethical principles, practices and virtues of emergency response can be pursued in a number of ways and IT can support or obstruct their realisation. Several dimensions of influence on the lawfulness, ethics, sociality and social responsibility of technologically augmented practice become visible:

- The ways in which technologies are used
- The technology itself
- The economic, social and cultural environment

Table 1. Ethical principles, practices and virtues and intended and unintended effects of IT use

Ethical Principles	Definition/Components of Service	Practices and Virtues	Some Effects of using IT
Humanity	• Prevent and alleviate suffering • Respect for and active protection of dignity • Particular attention to the vulnerable • Safeguard and restore environment and social ties	Compassion, charity, hope, empathy, resilience, respect, effective communication	Faster, more efficient and more informed response. Information overload for responders.
Impartiality	• Non-discriminating • Based on need • With neutrality, that is, without ideological debate	Non-judgement, tolerance, justice, fairness	Tireless, unbiased application of logic. Novel capabilities to identify vulnerable populations. Social sorting.
Solidarity	• Responsibilities and benefits shared equitably • Regardless of political, cultural, economic differences • Respect for sovereignty	Integrity, trustworthiness, respect, effective communication	Enhanced capabilities for communication and resource distribution. Potential for 'witchhunt' and spreading of rumours.
Cooperation	• Integration – e.g. with information sharing agreements • Inform & enable participation from all relevant parties • Direction – clarity of purpose • Subsidiarity	Prudence, improvisation, effective communication, respect, intersubjectivity, resilience	New ways of dynamically sharing information about capacities. Distributed collaboration makes it more difficult to know who is doing what.
Information Sharing	• Appropriate accuracy, precision, depth of detail • Consider effects of not sharing • Collect, process and share lawfully • Data minimization and sharing of aggregated data • Accountability & transparency • Evaluate effects on data subjects and informants • Avoid duplication	Prudence, integrity, trustworthiness, respect, empathy, effective communication	Enhanced technical interoperability can support compatibility between different information systems. Interfere with cultural and organisational practices.
Human Rights	• Rights to privacy, freedom of movement, association, expression are actively protected • Compulsory evacuation is explained	Prudence, respect, empathy, non-judgement, justice	Easier to contact and communicate with populations. Enhanced capabilities for information sharing can promote surveillance.
Preparedness	• Reduce vulnerabilities • Anticipation – e.g. through risk analysis & training • Continuity – grounded in familiar ways of working • Prepare for interoperability	Attitude of wisdom, prudence, respect, diligence, effective communication	Information visualisation and expert systems can augment human capabilities of risk analysis. Technology can introduce more complexity and slow people down.
Social contract	• Accountability to those in need, funders and society • Training and support for emergency responders	Prudence, respect, effective communication	Digital logging can make decisions more transparent. It can expose responders to unreasonable liabilities.

At every level both positive and negative effects can be produced, often simultaneously and in complex ways. The papers in this special issue provide concrete insight into the dynamics of this in a variety of different contexts.

CONCRETE INSIGHTS THROUGH IN-DEPTH STUDIES

Ellebrecht and Kaufman provide in-depth insight into some of the complexities of socio-technical effects through a study of e-triage. They elaborate a critique of pervasive claims that IT enables efficiency gains and thereby build a very useful foundation for all of the contributions to this special issue. Their argument is based on findings from a four-year research project in Germany, aimed at creating and implementing IT to support 'Immediate Rescue in Large-Scale Accidents with Mass Casualties' (SOGRO). Following actor network theories in the social sciences, Ellebrecht and Kaufman describe the work required to carry out triage and rescue in such situations as a complex programme of actions that is transformed in interaction with new technologies. During a series of large scale exercises they observed how the capabilities of digital triage technologies and their appropriation into practice were problematised by the emergency responders involved in the exercises. At the heart of the responders' experience are concerns with efficiency. The SOGRO system is promoted as a system that 'improves emergency treatment significantly by saving time, providing a more detailed situation overview and integrating the flow of information between all parties involved'. This is said to 'help save lives'. Ellebrecht and Kaufman focus on three areas of friction they observed: time savings, improved decision making capabilities, and the claim that the new technologies provide a comprehensive overview. They find that, in terms of time savings, the system responds to – and drives and further legitimizes – currently contested changes in the organization of triage in German emergency response organizations. There are two elements. Firstly, in Germany, mass casualty incident triage was traditionally carried out by physicians and documented by paramedics. This is a costly, labour intensive and relatively slow practice with high quality standards. SOGRO supports paramedic triage, that is, a shift of responsibility from emergency physicians to (cheaper and more numerous) paramedics, who can be prompted or strictly guided by a 'simple triage and rapid treatment' protocol (START) captured in an algorithm that takes the paramedic through a series of diagnostic steps. Secondly, the SOGRO system enables a shift from traditional practices of treating victims at the incident site to a 'scoop and run' technique that prioritise transporting victims over on-site treatment, seeking to facilitate treatment en-route and in available hospitals and treatments centres through dynamic, computationally augmented analysis of capacity and resources. Based on their analysis, Ellebrecht and Kaufmann argue that any efficiency gains that are generated at this contexture of social, organizational and technical innovation reflect the 'co-constitution of technology and society' rather than any simple technology based improvement. Moreover, the changes explored during these exercises remain contested, especially with a view to questions about the quality of care and judgement in the comparison between the two different modes of practice. Ellebrecht and Kaufman find similarly complex ambiguities in relation to claims of technology 'providing' an overview and enhancing decision making capabilities. Particularly remarkable are their observations on responders' worries about increased transparency in relation to professional liability law suits. In a survey of participants 76.6% of surveyed paramedics agreed with the statement that they 'occasionally had one foot in prison'. Unintended consequences of such concerns could be a lack of willingness to take risky decisions which could risk lives. By highlighting a series of ambiguities arising in the co-constitution of technology and society, Ellebrecht and Kaufmann's study sensitises the reader to the entanglement of social practice, societal values and technological potential.

Ford, Stephens and Ford call for circumspect attention to a different set of unintended consequences in relation to organizational policies of banning mobile devices and their impact on crisis communication. They show that while some employees, especially knowledge workers, may be expected to carry mobile devices 24/7 to stay connected with their colleagues and managers, others are prohibited from using or even carrying their personal mobile devices. In crisis situations this can lead to severe communication difficulties. Ford, Stephens and Ford carried out focus group discussions with 46 participants from two very different organizations where such mobile device bans were in place and found many examples of lost information, disconnected and even forgotten workers, isolated and hard to locate. The employees of a fast food company and a company providing cleaning and janitorial services reported frequently missing critical information, for example about emergency drills. Their supervisors were so overwhelmed with the need to coordinate selective information flows that they missed informing some of their workers altogether, even in emergencies. In one situation, the distributed janitorial workforce was not informed of a severe weather event until all public transport had been suspended. While their supervisors, secretarial and managerial colleagues had been informed in a timely manner and were safely ensconced at home, cleaning crews and janitors were stranded and without means of communication. Apart from putting workers in discomfort or even danger, organizational policies and practices of banning mobile devices create experiences of inequality and relative deprivation, which are harmful to workers' sense of well-being and justice. They can also undermine their loyalty to the company. Overall, the study reveals that there are complex digital inequalities and varying degrees of access to technology beyond socio-economic determinants that have a significant impact on crisis communication. Far from being a binary, mostly economically defined distinction between digital haves and have-nots and physical/economic access to technology, the digital divide can be a temporary, structurally defined, humiliating and unequally risk-laden experience.

In their article 'Ethical and Privacy Implications of the Use of Social Media During the Eyafjallajokull Eruption Crisis', Watson and Finn broaden the focus on organizational policies on digital communications by examining information flows between corporations and their customers during the most severe global flight disruption since 9/11. With over 100,000 flights cancelled and 1.2 million passengers affected, the particle cloud generated by the Eyafjallajokull eruption in 2010 overwhelmed corporate and institutional call centres. Stranded and unable to find information through official channels, thousands of passengers, their colleagues, friends and family turned to social media. Through a study of two different forms of support for information exchange using social media, Watson and Finn highlight positive outcomes such as increased surge capacity and the mobilisation of social capital, but also explore problematic issues of inequality, exploitation and privacy infringement. The site 'Stranded in Europe' was created by an Ericson employee to support self-organised information exchange between travellers, combining SMS messaging and Facebook. This greatly broadened access to the service. Once travellers had found the service using the Internet, the site allowed them to seek and exchange information via SMS, without the need for an online connection. This enhanced individuals' resilience by improving the prospect of gaining correct information from fellow travellers faster and more reliably than other sources allowed, and supported a creative response to the crisis. In some cases, information provided by people affected was also useful for professional emergency responders, reflecting a broader trend towards integrating social media information into crisis response efforts. In parallel, many umbrella organisations – such as the European Organisation for the Safety of Air Navigation – as well as individual airlines, travel agents and service providers offered corporate or institutional information services using social media, from Youtube to Twitter and Facebook.

Many gained thousands of new followers and fans through these services within days, and they used these channels in three ways: as a broadcast medium, as a means for direct communication with customers, and as a means to crowdsource information from customers. Watson and Finn highlight that this corporate turn to social media was highly effective, but also problematic in a number of ways. First, those unable to access digital technologies were 'disproportionately impacted by their inability to gather information and communicate' in the absence of appropriate levels of offline information services. Corporations and institutions sometimes provided online services instead of traditional services such as staff on the ground or in call centres. Second, the corporate practices created information asymmetries where those who were able to access online resources were often unaware that personal information they provided to gain support (name, age, location) could later be used or passed on to other operators to target advertising. Even if they did know, there often was no alternative source of information, eroding expectations of privacy and notions of consumer consent. Corporations also exploited consumer and public labour, effectively 'outsourcing' some aspects of their information services. Watson and Finn call for deeper critical reflection before social media are deployed in crisis response and management – be it through corporations or in the context of official efforts. They call for designers to be aware of opportunities and challenges as well as grassroots 'social hack' innovations such as the use of a #noshare hashtag to control the sharing of personal information, because greater sensitivity may avoid the need for costly retrofits on technologies designed without circumspection for ethical, legal and social issues.

In the contribution by Rizza, Guimarães Pereira and Curvelo we see that debates on ethical, legal and social issues are often dominated by concerns over privacy and data protection. The authors challenge this overly narrow conception of ELSI with a study of "Do-it-yourself justice" following the 2011 Vancouver riots. As the Vancouver Canucks were losing against the Boston Bruins during the 2011 Stanley Cup, some groups watching the game on large screens in the city began to orchestrate riots that lasted for several hours, lighting fires and destroying cars and property in the centre of Vancouver. The public reacted angrily to the destruction and when Vancouver Police Department (VPD) issued a call for help in identifying rioters on different social media platforms, they reacted with great energy. This public support had the potential to enhance collaborative resilience, and images submitted or tagged by members of the public led to hundreds of convictions, but it also sparked attempts at vigilantism and 'do-it-yourself justice'. This, in turn, sparked a lively and very critical debate within traditional media and Rizza, Guimarães Pereira and Curvelo use frame-analysis to identify key ethical, legal and social issues in public discourses articulated in the media. This analysis reflects potent imaginaries and fears circulating amongst the public, the emergency services and governing authorities. Rizza, Guimarães Pereira and Curvelo identify a range of such concerns, including a lack of legal regulation for the use of evidence generated by engaging citizens via social media in criminal investigations. The authenticity, completeness and reliability of the evidence could be seen as questionable in some cases and this should have affected its admissibility in court, but did not, in some cases. The media suggest that VPD were seduced by the potential of social media communication with the public, and acted without considering how they would deal with the results. This is framed as a matter of institutional unpreparedness and linked to the spread of unintended forms of do-it-yourself justice, and wider societal consequences such as a slide into an 'unintended "do-it-yourself" society' where mob behaviour and vigilantism are allowed to exacerbate oppressive tendencies within a surveillance society. Social media become 'leaky containers' in this maelstrom, mixing public and private, official and social in new ways and making criminal investigation part of social interactions. Citizens became empowered as surveillors of others and as judges

of deviance in ways that spun out of control. By presenting an analysis of these challenges to justice, fairness, responsibility, accountability and integrity, Rizza, Guimarães Pereira and Curvelo scrutinize complex reverberations of using social media in crises and enable a critical engagement with wider societal implications of socio-technical innovation in the relationship between the emergency services, legislative and judiciary governance and public engagement.

Tapia and LaLone's study 'Crowdsourcing Investigations: Crowd Participation in Identifying the Bomb and Bomber from the Boston Marathon Bombing' explores some of the issues raised by Rizza, Guimarães Pereira and Curvelo in greater depth as well as analysing how traditional media contributed to ethical dilemmas. Two years after the events in Vancouver, the social media response to the Boston Marathon – in part encouraged by the FBI, in part self organised through leading social media groups like *Reddit* and *Anonymous* – revealed that the frontier land of crowd participation in criminal investigations still teems with ethical, legal and social frictions. Within hours of the Boston Marathon bombing, which killed four people and injured 264 others, the FBI called for bystanders to share images and video of the bombing. Online groups also responded to the events, trying to position themselves as hubs for self-organised investigations and crowdsourcing of information and support for survivors. The activities of two such groups, *Reddit* and *Anonymous* played a part in ethical lines being crossed during the crowdsourced investigation. By using sentiment analysis of public responses to the activities of *Reddit* and *Anonymous* expressed in over 23 million tweets, Tapia and LaLone are in a position to trace these moments when lines of ethical acceptability were crossed. They show that *Reddit*, in particular, attracted intensely emotional reactions, understandable as a highly charged public response to the highly charged nature of the events. To begin with, the colour of this emotion was overwhelmingly positive, reflecting public support for activities such as organising pizza and water for survivors and the Boston Police Department, or helping loved ones to contact known survivors. It was also seen as positive that *Reddit* provided timely and accurate news about the events, outshining mainstream media such as CNN. However, this assessment shifted radically, when *Reddit* spearheaded news that falsely identified two people as suspects and posted images of them, especially tragically wrongly blaming Sunil Tripathi, a teenager who had gone missing from his home and who was later found to have committed suicide. Public sentiment condemned this with comments that expressed very negative evaluations of the 'irresponsible amateur sleuthing' that had been encouraged by the online group. Tapia and LaLone discuss how these and other ethically problematic activities, were exacerbated by a lack of interaction between the official investigation teams at Boston PD and the FBI and a lack of judgement and restraint from mainstream media. Long established national media treated the online sources like news agencies, accepting and broadcasting 'news', including statements about Sunil Tripathi without questioning. Tracing public engagement in criminal investigations historically, Tapia and Lalone draw links between printed 'Wanted' posters, televised appeals and crime reconstructions and the use of social media for involving the public in criminal investigations. The 'remediations' or transformations that are associated with technological affordances in this current round of innovations seem significant. The crowd is without the training or understanding of ethical and legal constraints that professionals have, but it is equipped with more power and reach, especially when amplified through mainstream media, and Tapia and LaLone call for a reassessment of practices of crowdsourcing investigations that could have significant real-world implications in situations that demand 'socially responsible, careful, considered action'.

The final paper in this special issue examines transformations of privacy engendered in the context of socio-technical innovation in IT supported crisis response and management, especially when it is connected into smart city

technology. Büscher, Perng and Liegl question the common assumption that privacy and liberty must be sacrificed for security and explore design *for* privacy as an approach that can support people in finding a better balance between privacy and security. By identifying three key trends that underpin the informationalization of emergency response, they set the scene for a study of privacy as a lived practice of boundary management. First, there is great technological potential for gathering, sharing and utilising more information about populations and environments affected by, or at risk of, crisis. Second, people produce more personal information than ever before, richly and dynamically documenting their lives and the world around them through mobile technologies and interactions online. Third, real and perceived increases in risk have generated a 'culture of fear' that can be leveraged to justify surveillance, increased information sharing and preventative measures. People's capabilities to separate public and private have been transformed in this forcefield of innovative momentum and with this, democratic cornerstones of liberty, freedom, dignity and humanity have been worked loose. Current attempts to counterbalance this, for example through 'privacy by design', are inadequate. Privacy is not a binary state of either withdrawal into a sealed private sphere or transparent public exposure, but a practically achieved and contextual matter of far more diversified boundary management. What is to be made public or kept private changes depending on what role one is in and what dimensions of time and space are involved. Fire fighters may be willing to share intimate physiological data about their breathing with colleagues, they might need to manage disclosure of their precise location to other responders in the course of the unfolding response, and they might happily disclose such information in an anonymised form for future training simulations. New technologies and practices of their appropriation have turned documentary records of entire populations' physiological data, movements, communications and social networks into indentifying personal information as precise as fingerprints. These new affordances make it difficult for people to control the spread and use of personal information, especially given the often silent and invisible operation of technologies that analyse such data. A range of challenges arise here around the spread of surveillance, social sorting, an erosion of civil liberties, and a securitization of everyday life. To respond proactively to these challenges and the transformations of people's capacities to modulate privacy, Büscher, Perng and Liegl question the use of 'privacy by design' approaches, specifically their aim to 'hardwire' compliance with regulations into technologies. In the context of emergency response, where role improvisation, creativity and flexibility as well as clear discipline and procedures are essential aspects of effective practice, and where 'emergent interoperability' and ad-hoc assemblies of systems of systems are a powerful possibility, it seems more promising to focus on designing *for* material and social practices of privacy boundary management. Such human practice based approaches can respond more directly and more carefully to the opportunities and challenges inherent in the positively and negatively disruptive innovation that shapes the future of crisis response and management.

These concrete explorations can help us understand better how ethics is distributed between people, technology, and the economic, social and cultural environment. Core questions for analysts, designers and practitioners involved in IT innovation in crisis response and management are how does technology become ethically problematic or "good"? and how might we control this? when 'the multistable nature of artefacts means that they may become used in ways never anticipated by the designers or originators' (Introna 2007:16). Furthermore, in many societies, ethics has become pluralized, and ethical values are relative and subject to dynamic processes of change and negotiation over time. Such change should be the subject of open democratic debate (Rawls, 1971; Habermas, 1996) and for that to happen, ethical issues have to be noticed and turn from matters of fact, that is, accepted, unnoticed, taken for granted, common-sense facts of life, into 'matters of

concern', that is, interrogated, dissected, contested objects of critique (Latour, 2005). Another key question for an ethically circumspect approach to IT innovation in information societies therefore is how to make ethical opportunities, challenges and risks public? and how to engage and include (which?) stakeholders?

Unless technology is analysed and made as one element within a nexus of values, practices and 'environmental' conditions, unintended consequences are likely to be hard to notice and know in sufficient detail soon enough, to anticipate, mitigate or avoid. Introna and Wood argue that:

...the politics of technology is more than the politics of this or that artefact. ... we cannot with any degree of certainty separate the purely social from the purely technical, cause from effect, designer from user, winners from losers, and so on. (2004, 179)

A range of methodologies exist that respond to these challenges, including responsible research and innovation (Von Schomberg, 2013), collective experimentation (Wynne & Felt, 2007), disclosive ethics (Introna 2007), value sensitive design (Friedman, Kahn & Boring, 2006), co-realization (Hartswood, Procter, Slack, Voß, Buscher, Rouncefield, & Rouchy, 2002) and 'design after design' (Ehn, 2008). We will briefly discuss these in relation to a roadmap of future work that concludes this introduction. However, before we do so, it is necessary to acknowledge that the 'multistable' nature of technologies does not mean that they can be used in any which way users deem appropriate. Technology is not neutral nor endlessly malleable. It actively enacts and shapes morality. By summarising an exemplary disclosive ethics enquiry into technological moral effects and adding this to the collection of studies compiled in this special issue, we seek to sharpen the senses even further to the fluid morality and politics of IT innovation in crisis response and management, a domain where morality matters perhaps more than anywhere else, because crises can set precedents that may seep into normality with far-reaching consequences.

Disclosive Ethics: Morality and Facial Recognition Systems

Two contributions to this special issue explore how social media technologies have been used by local authorities, police and citizens to identify persons during the 2010 Vancouver riots (Rizza et al.) and the 2013 Boston bombing investigations (Tapia and LaLone). Alongside such innovation, since 9/11 there has been an increase in investment in face recognition systems (Introna and Wood 2004, Gallagher 2013). They compare images of the faces of people captured by video or still cameras with a database of images of faces. The functionality is threefold:

- Verification: Are you who you say you are?
- Identification: Who are you?
- Watch list comparison: Are we looking for you? (Phillips, Grother, Michaels, Blackburn, Elham & Bone 2003:6)

The system presents matches to human operators and, when watchlist monitoring, it can highlight matches to persons who are wanted - 'bad guys' in a sketch by Phillips et al (2003). For crisis management and emergency response, Facial Recognition Systems have been used for preventive policing to avert crises. For example, during the London 2012 Olympics, the already famed London CCTV infrastructure was extended with facial recognition software and London became 'the most watched Olympic Games in modern history, but not just in the traditional sense of sporting spectators' (Army Technology, 2012). The US Department of Homeland Security is currently testing Face Recognition Systems with audiences and volunteers at mega sports events. This interest is based on expectations that such systems may be useful in the emergency response phase, for example to identify perpetrators during or in the immediate aftermath of violent attacks or for victim identification (Gevaert & de With,

2013). In an experiment, researchers at Michigan State University were able to identify one of the Boston Marathon bombing suspects from law enforcement video (Klontz & Jain, 2013, although see Gallagher 2013 for a discussion on how facial recognition failed in this instance).

Advantages of such systems over human face recognition practices are the number of faces that can be processed in this way, and the impartial, tireless and consistent application of procedures. Indeed, face recognition is often hailed as less biased than humans. Introna and Wood cite statements not only from manufacturers and vendors, but also from prominent security forums, such as 'Face recognition is completely oblivious to differences in appearance as a result of race or gender differences' (2004:191). In light of concerns over social sorting and discrimination especially against Muslim populations in security measures (Vertigans 2010) such promises are powerful incentives for ethically and socially responsible innovation champions. However, closer inspection actually reveals bias to be an integral part of the technology. A 2002 Face Recognition Vendor Test of the most powerful algorithms found, for example, that males were 6-9% points more likely to be identified than females (Phillips, cited in Introna and Wood 2004:190). Givens, Beveridge, Draper, & Bolme (2003) also find racial and age bias. Their experiments show that

Asians are easier [to recognize] than whites, African-Americans are easier than whites, other race members are easier than whites, old people are easier than young people (cited in Introna and Wood 2004:190)

This bias is not due to any intentionally built in weighting; it is accidental: A function of the absence of strong shadows on male faces as well as darker and older faces, the nature of images and their processing by this face recognition system. The problem is that being easier to recognize also makes being classed as a false positive and being exposed to investigations more likely. Thus, rather than being neutral, some Face Recognition Systems can (unintentionally) amplify political, cultural, and institutional forms of discrimination. At this juncture it becomes clear that morality is not purely human but effected by collectives of humans, technologies, and socio-economic and political circumstances, 'what Foucault called dispositifs' (Latour, in Introna 2007:13), and technology can can play an active part in its own right if it is not designed with careful attention to unintended consequences. There is, in this example, no clearly identifiable single human or technological responsible agency for morally problematic effects of discrimination: 'there is often nobody there that "authored" it as such' (ibid), rather, there can be a Kafkaesque culmination of indifference, error, abuse, lack of transparency and accountability (Solove 2001) that leads into moral dilemmas.

A lack of transparency is particularly critical. Disclosive ethics is a methodology that seeks to enable analysis of how seemingly trivial details (such as the capacity of optical mechanisms to process the light-reflective quality of different types of skins) can turn into politics and become tied to, and amplified through other exclusionary practices (such as political and cultural prejudice stoked by a rhetoric of a 'war on terror'), so that 'what seems to be a rather trivial injustice soon may multiply into what may seem to be a coherent and intentional strategy of exclusion' (Introna & Wood 2004:179). The method proceeds by showing that many digital technologies are silent as opposed to salient technologies and opaque as opposed to transparent (Introna & Wood, 2004:183).

Facial recognition is a particularly striking example of a silent technology since it can be imbedded into existing CCTV networks, making its operation hard to notice. Furthermore, it is passive in its operation. It requires no participation or consent from its targets. The process is obscure, 'non-intrusive, context-free', based on software algorithms that are proprietary, making it difficult to get access to them for inspection and scrutiny. Moreover, these algorithms are so complex that even experts can struggle to interpret and understand them. As a result, 'for

Table 2. Silent/Salient Technology (Introna &Wood 2004:183)

Silent Technology	Salient Technology
Embedded/hidden Passive in its operation (limited user involvement) Application flexibility (open ended) Obscure (form/operation/outcome) Mobile (software)	On the 'surface'/conspicuous Active in its operation (fair user involvement Application stability (firm) Transparent (form/operation/outcome) Located (hardware)

most ordinary members of society, facial recognition systems are an obscure "black box"' (Introna & Wood 2004:183).

The lesson from this example of disclosive ethics is that morality is not simply human. Agency, intentionality and ethics are distributed within socio-technical systems, and it is the particular way of 'working together' that makes a certain collective or network of humans, environments and technologies have (un-)intended, potentially undesirable ethical effects. It would, therefore, be short-sighted to think of technology as neutral, and to look for the ethics of action solely in the way people use technology. Technology can be employed with benign intention, yet turn out to have ethically, legally or socially undesirable effects. It is critical that the fact that just this technology in just these circumstances produces discriminatory effects should be notice-able and it should be possible for this effect to be made into a matter of concern. This is in no way a technology deterministic reading, where we claim that technology is a 'culprit'. Quite the opposite, even though it is not so in this case, it could just as well be the technology that is correcting human bias (Latour & Venn, 2002). The consequence however has to be that efforts are made to 'subject [technological] artefacts to the same level of scrutiny' (Introna & Wood 2004: 195) as humans and to find approaches (in best practice, legal regulation and design) to ensure the scrutinizability socio-technical collectives, especially in ethically highly charged areas such as security or emergency response.

DOING IT MORE CAREFULLY: FUTURE WORK

In the different, but related context of designing 'solutions' to address ecological crisis, Bruno Latour argues 'We have to be radically careful, or carefully radical.' (Latour, 2008, 7). Supporting awareness of ELSI and practices of addressing them in IT supported crisis response and management is another extremely complex challenge, in a highly sensitive and important domain for contemporary societies, and we would say we need to be *both:* radically careful and carefully radical. Analysts, designers, and practitioners must not only take responsibility for (the inevitability of) unintended consequences with careful circumspection, they must also formulate and pursue ambitious, perhaps radical socio-technical critique and creativity. The contributions to this special issue and the discussion in this introduction map out a large terrain for research and design, with some areas uncharted and others skillfully cultivated, but isolated from each other. In this concluding section we suggest a roadmap for research to develop studies that explore the unknown and connect research in different subject areas and disciplines (ethics, law, practice, social science, philosophy, anthropology, organizational studies, design, computing), all with a view to informing more careful and circumspect, yet also ambitious and 'radical' ELSI aware socio-technical innovation.

First of all, research is needed that explores existing ethical, legal and social issues in emer-

gency response and management with a view to how technologies might be designed and constructively inserted to address opportunities and challenges. Campbell's *Library of Essays on Emergency, Ethics, Law and Policy* (2012), reflective practitioner reports (such as Larkin's review of the international Haiti response 2010), post disaster reviews, or investigations into specific challenges, such as Weick's seminal study of the failure of leadership and sense-making in the Mann Gulch Disaster (1993), Cole's analysis of interoperability (2010) or the UK government's advice on data sharing in emergencies (Armstrong, Ashton & Thomas, 2007) can serve as a quarry for inspiration, but there is a need for more concrete and rich narratives and descriptions of ethical, legal and social issues as they are encountered in practice.

Secondly, more studies are needed of how the design and appropriation of new technologies generate known and 'new' ELSI – such as a preference for 'remote control'. They should explore how these might be addressed through innovative engineering and design as well as innovative use and organizational policies. Thirdly, a large range of methodologies exists for noticing ELSI and for folding critical and creative ELSI awareness into innovation. They currently exist in isolated pockets and include different approaches that can sensitize researchers, designers and practitioners to ELSI and different design methodologies. Sensitizing approaches are, for example:

- **Privacy Impact Assessment and Ethical Impact Assessment:** Designed to be embedded in innovation processes, based on iteratively probing for ELSI through systematic questioning of stakeholders about the use and design of technologies (Wright 2011).
- **Value Sensitive Design:** A theoretically grounded approach to integrating concern for human values in a principled and comprehensive manner throughout the design process, based on a tripartite methodology, consisting of conceptual, empirical, and technical investigations (Friedman et al, 2006).
- **Computer Supported Cooperative Work:** An interdisciplinary research field that integrates insights from in-depth qualitative studies of collaborative work, often using ethnographic methods into the design of computer systems (Schmidt & Bannon, 1992, Suchmann, [1987] 2007)
- **Science and Technology Studies:** A prolific, philosophically and sociologically oriented interdisciplinary endeavour to understand the dynamic relationship between science, technology, society and human practice (Bijker & Law, 1992)
- **Responsible Research and Innovation (RRI):** A guiding concept for European funded research, technology development and management, aiming to ''better align both the process and outcomes of R&I, with the values, needs and expectations of European society.'' (European Commission 2014, Von Schomberg, 2013).
- **Software Studies:** A relatively new field, where researchers explore how algorithms and computational logic function and 'leak out' of the domain of computing into everyday life and examine 'the judgements of value and aesthetics that are built into computing', and the subcultures and politics of programming (Fuller, 2008).

Methods of designing in an ELSI aware manner include

- **Privacy by Design:** An approach with several meanings and origins, specifically focused on preserving privacy (Cavoukian, 2001; Langheinrich, 2001). Firstly, privacy by design is about heightening sensitivity to privacy issues during design. Secondly, it can be about enforcing compliance with privacy regulations through hard wiring constraints on practices into design with privacy enhancing technologies (PETs). Existing examples include privacy policy inspection, access control restriction, and pseudonymisation tools (Pearson, 2009).

- **Collaborative Design (Co-Design):** A form of participatory design, and broadly motivated approach to address ethical and social aspects of IT innovation, focused on utilising diverse forms of expertise through engaging stakeholders as co-designers from the earliest stages of design. The process is iterative and based around prototypes (Greenbaum & Kyng, 1991).
- **Co-Realization:** Develops ideas of Co-Design through a synthesis of ethnomethodology (a particular form of sociological enquiry) and participatory design. It moves the locus of design and development activities into workplace settings where technologies will be used, emphasises design-in-use and longitudinal involvement of IT professionals in the 'lived work' of users (Hartswood et al. 2002).
- **Critical Design:** Also know as 'design noir' (Dunne & Raby 2001) or 'speculative design' (Sengers and Gaver 2006) straddles into art and philosophy as it seeks to provoke and enable critical engagement. It creatively and critically explores putative futures entailed in contemporary technological developments, often by creating objects that are obliquely functional but also absurd or shocking.
- **Service Design:** Arelatively new approach, focused on designing 'services' – assemblages of human, technological, architectural, organizational components (Meroni & Sangiorgi, 2011).
- **Collective Experimentation:** A 'new regime' of technoscientific innovation, characterised by experimental implementation of new technologies in the context of broad-based stakeholder engagement. It requires new approaches to intellectual property rights to ensure viability (such as Open Source Software, General Public Licence (GPL or copyleft) and 'new forms of interaction between scientists and other actors, … because the traditional authority of laboratory-based science is not sufficient' (Wynne & Felt, 2007, 27).
- **Design for Design:** An approach that recognises that design does not end at 'design time'. People appropriate technologies in a way that constitutes 'design in use'. This is often ill supported by silent technologies and blackboxing. 'Design for design' seeks to support people in developing the skill and understanding needed to be creative with technology as well as knowing about the effects of using technologies in particular ways (Ehn, 2008, see also work discussed in Büscher, Perng & Liegl, this issue)

There are overlaps, synergies, as well as incompatibilities between these approaches and there are no doubt more relevant approaches than those listed here. What a list like this makes plain, however, is that overviews, review essays and handbooks are needed that draw together the best from these different methods, prevent researchers, designers and practitioners from re-inventing the wheel and enabling them to develop synergies, to make the work cumulative, not isolated. Reviews should aim to support mixed methods – not standardisation. In addition, reflective analyses of successful attempts and troublesome trajectories in employing these methods would be useful, especially if they are not focused not on the methods for methods' sake, but the aims, practices and outcomes of responsible research and innovation.

Finally, we need studies that review and discuss the state of the art in ELSI innovation in IT as well as law, policy and organizational practice, for example privacy preserving techniques that can support multi-agency information sharing (see Büscher, Perng and Liegl, this issue), usage and image retention restrictions and public notice obligations for the use of RPAS and innovative ways of supporting accountable data flows (Cavoukian, 2012, Bracken-Roche, Lyon, Mansour, Molnar, Saulnier & Thompson, 2014), clarification of liabilities emergency agencies may incur when using automation and remote controlled devices (Holloway, Knight, & McDermid, 2014) or utilising citizen data (Bailey Smith 2014). What regulatory instru-

ments, technologies, social or organizational innovations could support more responsible and circumspect emergency response and management? What exists? How does it work? How could it be used? What is missing?

We hope you enjoy reading the papers in this special issue and feel inspired to contribute to this exciting field of research in the future.

Monika Büscher
Michael Liegl
Caroline Rizza
Hayley Watson
Guest Editors
IJISCRAM

REFERENCES

Aradau, C., & Van Munster, R. (2011). *Politics of Catastrophe: Genealogies of the Unknown*. London: Routledge.

Armstrong, H., Ashton, C., & Thomas, R. (2007). *Data Protection and Sharing – Guidance for Emergency Planners and Responders*. *Office*. London. Retrieved from www.cabinetoffice.gov.uk/media/132709/dataprotection.pdf [Accessed 31 December 2014]

Army-Technology.com. (2012). Keeping London's Olympic Games secure on all fronts - Army Technology. http://www.army-technology.com/features/featurelondon-2012-olympics-games-security-strategy/ [Accessed 30 December 2014]

Bailey Smith, J. D. (2014). *Agency Liability Stemming from Citizen-Generated Data*. Retrieved from http://www.wilsoncenter.org/publication/agency-liability-stemming-citizen-generated-data

Barnard-Wills, D. (2013). Security, Privacy and Surveillance in European Policy Documents. *International Data Privacy Law*, *3*(3), 170–180. doi:10.1093/idpl/ipt014

Bech Gjørv, A. (2012). Rapport fra 22 Juli-Kommisjonen. Oslo. http://www.regjeringen.no/smk/html/22julikommisjonen/22JULIKOMMISJONEN_NO/INDEX.HTM [Accessed 22 August 2014]

Beck, U. (1992). *Risk Society: Towards a New Modernity*. London: Sage.

Bijker, W., & Law, J. (1992) (Eds.), Shaping Technology, Building Society: Studies in Sociotechnical Change. Cambridge, Mass.: MIT Press.

Bracken-Roche, C., & Lyon, D. MAnsour, M. J., Molnar, A., Saulnier, A., & Thompson, S. (2014). *Surveillance Drones: Privacy Implications of the Spread of Unmanned Aerial Vehicles (UAVs) in Canada*. Kingston. http://www.atlanticuas.ca/files/Library/Reference/Privacy Implications of the Spread of UAVs in Canada_14-04-30.pdf [Accessed 30 December 2014]

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. doi:10.2202/1547-7355.1252

Campbell, T. (2012). *The Library of Essays on Emergency, Ethics, Law and Policy: 4 Volume Set*. Farnham: Ashgate.

Cartlidge, E. (2012). Aftershocks in the courtroom. *Science*, *338*(6104), 184–188. doi:10.1126/science.338.6104.184 PMID:23066054

Cavoukian, A. (2001). Taking Care of Business: Privacy by Design. Toronto. http://www.ontla.on.ca/library/repository/mon/2000/10296375.pdf [Accessed 25 Nov 2012]

Cavoukian, A. (2012). *Privacy and Drones: Unmanned Aerial Vehicles*. http://www.ipc.on.ca/images/Resources/pbd-drones.pdf [Accessed 30 December 2014]

Chesbrough, H. W. (2003). *Open Innovation: The New Imperative for Creating and Profiting from Technology*. Boston: Harvard Business school Press.

Cole, J. (2010). *Interoperability in a Crisis 2. Human Factors and Organisational Processes*. http://www.rusi.org/downloads/assets/Interoperability_2_web.pdf [Accessed 17 February 2014]

Committee of Public Accounts. (2011). Public Accounts Committee - Fiftieth Report The Failure of the FiReControl Project HC 1397. London. http://www.publications.parliament.uk/pa/cm201012/cmselect/cmpubacc/1397/139702.htm [Accessed 28 October 2014]

Ehn, P. (2008). Participation in design things. In *PDC '08 Proceedings of the Tenth Anniversary Conference on Participatory Design 2008, Indiana University* (pp. 92–101). Indianapolis. eScience. (2012). Earth Faces a Century of Disasters, Report Warns. http://esciencenews.com/sources/the.guardian.science/2012/04/26/earth.faces.a.century.disasters.report.warns [Accessed 28 October 2014]

European Commission. (2014). Science with and for society. http://ec.europa.eu/programmes/ horizon2020/en/h2020-section/science-and-society. [Accessed 28 October 2014]

Friedman, B., Kahn, P. H., & Boring, A. (2006). Value Sensitive Design and Information Systems. In P. Zhang & D. Galetta (Eds.), *Human-Computer Interaction in Management Information Systems: Foundations*. New York: M.E. Sharpe.

Fuller, M. (2008). *Software Studies: A Lexicon*. Cambridge, MA: MIT Press. doi:10.7551/mitpress/9780262062749.001.0001

Gallagher, S. (2013). Why facial recognition tech failed in the Boston bombing manhunt |. Ars Technica. http://arstechnica.com/information-technology/2013/05/why-facial-recognition-tech-failed-in-the-boston-bombing-manhunt/ [Accessed February 16, 2014]

Gevaert, W. J. R., & de With, P. H. N. (2013, February 19). Robust face recognition algorithm for identifition of disaster victims. *Proc. SPIE* 8655, Image Processing. *Algorithms and Systems*, *XI*, 865503. doi:10.1117/12.2001634

Greenbaum, J. M., & Kyng, M. (1991). *Design at work: Cooperative design of computer systems*. Hillsdale, NJ: L. Erlbaum Associates Inc.

Habermas, J. (1996). *Between Facts and Norms. Contributions to a Discourse Theory of Law and Democracy*. Cambridge: MIT Press.

Hartswood, M., Procter, R., Slack, R., Voß, A., Büscher, M., Rouncefield, M., & Rouchy, P. (2002). Co-realisation: Towards a Principled Synthesis of Ethnomethodology and Participatory Design. *Scandinavian Journal of Information Systems*, *14*(2), 9–30.

Hollnagel, E., & Woods, D. D. (2005). *Joint Cognitive Systems: Foundations of Cognitive Systems Engineering*. Boca Raton: CRC Press. doi:10.1201/9781420038194

Holloway, C. M., Knight, J. C., & McDermid, J. A. (2014). Neither Pollyanna nor Chicken Little: Thoughts on the Ethics of Automation. In *IEEE International Symposium on Ethics in Engineering, Science, and Technology; 23-24 May 2014; Chicago, IL; United States*. Retrieved from http://ntrs.nasa.gov/search.jsp?R=20140010015 [Accessed 30 December 2014]

Introna, L. (2007). Maintaining the Reversibility of Foldings: Making the Ethics (Politics) of Information Technology Visible. *Ethics and Information Technology*, *9*(1), 11–25. doi:10.1007/s10676-006-9133-z

Introna, L., & Wood, D. (2004). Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems. *Surveillance & Society*, *2*(2/3), 177–198.

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). White Paper prepared for the Ethics Subcommittee, Advisory Committee to the Director, Centers for Disease Control and Prevention, Atlanta. http://www.cdc.gov/od/science/integrity/phethics/docs/White_Paper_Final_for_Website_2012_4_6_12_final_for_web_508_compliant.pdf [Accessed 31 December 2014]

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.

Klontz, J. C., & Jain, A. K. (2013). A Case Study on Unconstrained Facial Recognition Using the Boston Marathon Bombings Suspects. http://www.cse.msu.edu/rgroups/biometrics/Publications/Face/KlontzJain_CaseStudyUnconstrainedFacialRecognition_BostonMarathonBombimgSuspects.pdf [accessed 16 February 2014]

Koua, E. L., MacEachren, A. M., Turtun, I., Pezanowski, S., Tomaszewski, B., & Frazier, T. (2010). Conceptualizing a User-Support Task Structure for Geocollaborative Disaster Management Environments. In B. van de Walle, M. Turoff, & S. Hiltz (Eds.), *Information Systems for Emergency Management* (pp. 254–278). New York: Sharpe.

Langheinrich, M. (2001). Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems. *Proceeding UbiComp '01 Proceedings of the 3rd international conference on Ubiquitous Computing*, pp. 273-291. doi:10.1007/3-540-45427-6_23

Larkin, G. (2010). Unwitting partners in death-the ethics of teamwork in disaster management. *The Virtual Mentor : VM*, *12*(6), 495–501. doi:10.1001/virtualmentor.2010.12.6.oped1-1006 PMID:23158454

Lash, S., & Urry, J. (1994). *Economies of Signs and Space*. London: Sage.

Latour, B. (2005). From Realpolitik to Dingpolitik or How to Make Things Public. In B. Latour & P. Weibel (Eds.), *Making Things Public-Atmospheres of Democracy* (pp. 1–31). Cambridge, MA: MIT.

Latour, B. (2008). A Cautious Prometheus? A Few Steps Toward a Philosophy of Design (with Special Attention to Peter Sloterdijk). In F. Hackney, J. Glynne, & V. Minton (Eds.), *Networks of Design Proceedings of the 2008 Annual International Conference of the Design History Society (UK) University College Falmouth, 3-6 September*. Boca Raton: BrownWalker Press, 2-10.

Latour, B., & Venn, C. (2002). Morality and Technology: The End of the Means. *Theory, Culture & Society*, *19*(5-6), 247–260. doi:10.1177/026327602761899246

Letouzé, E., Meier, P., & Vinck, P. (2013). Big Data for Conflict Prevention: New Oil and Old Fires. In F. Mancini (Ed.), *New Technology and the Prevention of Violence and Conflict* (pp. 4–27). New York: International Peace Institute.

Meroni, A., & Sangiorgi, D. (2011). *Design for Services*. Farnham: Gower.

Merton, R. K. (1936). The Unanticipated Consequences of Purposive Social Action. *American Sociological Review*, *1*(6), 894–904. doi:10.2307/2084615

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. doi:10.1093/jopart/mun033

Palen, L., Vieweg, S., Sutton, J., & Liu, S. B. (2009). Crisis Informatics : Studying Crisis in a Networked World. *Social Science Computer Review*, *27*(4), 467–480. doi:10.1177/0894439309332302

Pearson, S. (2009). Taking Account of Privacy When Designing Cloud Computing Services. 2009 *ICSE Workshop on Software Engineering Challenges of Cloud Computing*, pp. 44-52. doi:10.1109/CLOUD.2009.5071532

Phillips, J. P., Grother, P., Michaels, R. J., Blackburn, D. M., Elham, T., & Bone, M. (2003). Face Recognition Vendor Test 2002. Overview and Summary http://biometrics.nist.gov/cs_links/face/frvt/FRVT_2002_Overview_and_Summary.pdf

Presentation at http://www.biometrics.org/bc2002/Phillips.pdf [Accessed 16 February 2014]

Rawls, J. (1971). *A Theory of Justice*. Oxford.

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

Sessions, R. (2009). The IT Complexity Crisis: Danger and Opportunity. https://dl.dropboxusercontent.com/u/97323460/WebDocuments/WhitePapers/ITComplexityWhitePaper.pdf [Accessed 28 October 2014]

Shapiro, D. (2005). Participatory Design: The Will to Succeed. *Proceedings of the 4th Decennial Conference on Critical Computing: Between Sense and Sensibility*, Aarhus, Denmark — August 21 - 25, 2005, 29–38. doi:10.1145/1094562.1094567

Solove, D. J. (2011). *Nothing to Hide: The False Tradeoff Between Privacy and Security*. New Haven: Yale University Press.

Suchman, L. (2007). *Human-Machine Reconfigurations* (p. 314). Cambridge University Press.

Thrift, N. (2005). *Knowing Capitalism*. London: Sage.

Thrift, N. (2011). Lifeworld Inc—and what to do about it. *Environment and Planning. D, Society & Space*, *29*(1), 5–26. doi:10.1068/d0310

van de Walle, B., Turoff, M., & Hiltz, S. R. (Eds.), *Information Systems for Emergency Management*. New York: Sharpe.

Vertigans, S. (2010). British Muslims and the UK Government's "War on Terror" Within: Evidence of a Clash of Civilizations or Emergent De-civilizing Processes? *The British Journal of Sociology*, *61*(1), 26–44. doi:10.1111/j.1468-4446.2009.01300.x PMID:20377595

Von Schomberg, R. (2013). A vision of responsible innovation. In R. Owen, J. Bessant, & M. Heintz (Eds.), *Responsible innovation* (pp. 51–74). London: Wiley. doi:10.1002/9781118551424.ch3

Weick, K. (1993). The Collapse of Sensemaking in Organizations: The Mann Gulch Disaster. *Administrative Science Quarterly*, *38*(4), 628–652. doi:10.2307/2393339

Wright, D. (2011). A framework for the ethical impact assessment of information technology. *Ethics and Information Technology*, *13*(3), 199–226. doi:10.1007/s10676-010-9242-6

Wynne, B., & Felt, U. (2007). *Taking European Knowledge Society Seriously*. Report of the Expert Group on Science and Governance to the Science, Economy and Society Directorate, Directorate-General for Research, European Commission. Directorate General for Research 2007 Science, Economy and Society. http://www.bmbf.de/pub/EuropeanKnowledge(6).pdf [Accessed 30 Dember 2014]

ENDNOTES

1 http://bssar.kemea-research.gr

2 http://www.tetratoday.com/news/tetras-love-affair-with-the-asia-pacific

Monika Büscher is Professor of Sociology at the Centre for Mobilities Research at Lancaster University. She researches the digital dimensions of contemporary 'mobile lives' with a focus on IT ethics and crises. In 2011, she was awarded an honorary doctorate by Roskilde University, Denmark. She edits the book series Changing Mobilities with Peter Adey.

Michael Liegl is Senior Research Associate at the Centre for Mobilities Research, Lancaster University. In his research he investigates the interplay of technology, spatial organization and social relations with a focus on the layering and hybridization of online and offline collaboration. Currently, he engages in domain analysis and participatory design and in the exploration of social, legal and ethical implications of IT supported emergency response in EU FP7 funded Bridge project http:/bridgeproject.eu/en*. Recent publications include: 'Digital Cornerville' (Lucius & Lucius 2010), and 'Nomadicity and the Care of Place' (Journal of CSCW 2014).*

Caroline Rizza, PhD is Associate Prof. in Information and Communication Sciences, in the Economics, Management and Social Sciences Department, Interdisplinary Institute on Innovation (i3) UMR – CNRS, Institut Mines Telecom/Telecom ParisTech (Paris, France); member of the Observatory for Responsible Innovation, and of the Chaire "Value and policy of personal data". From 2010-2014, she worked at the Joint Research Centre of the European Commission (Ispra, Italy) where she conducted research projects on "Ethics of Social Networks". Since then, her research has been focusing on the ethical, legal and social issues raised by emergent IT in specific situations such as interpersonal relations, crisis situations, ICT design (e.g. "privacy or ethics by design", "responsible innovation") and by special needs users. She is currently co-leading a research project on the "silence of the chips" concept in RFID for IoT contexts (CIPRIoT project funded by the Fondation Mines-Telecom and associated industrial partners) in collaboration with the JRC and the French CNRFID.

Hayley Watson, Senior Research Analyst, joined Trilateral in 2012. Her main area of expertise includes; the role of technology including social media in relation to security, and she is particularly interested in the use of ICT in crisis management. Prior to joining Trilateral, Hayley worked as a lecturer in sociology at Canterbury Christ Church University. She has published peer-reviewed journal articles on citizen journalism in relation to security and social media and crisis management. She is actively involved in the ISCRAM community (Information Systems for Crisis Response and Management) and co-chairs the ELSI track and working group on Ethical, Legal and Social Issues of IT supported emergency response. Hayley has a PhD in sociology from the University of Kent.