Privacy, Security, and Liberty: ICT in Crises

Accepted Version. Please cite as 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) 6(4): 72-92.*

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

Sung-Yueh Perng, National Institute for Regional and Spatial Analysis, National University of Ireland, Maynooth, Ireland

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

ABSTRACT This paper explores issues of privacy, security and liberty arising in relation to information and communication technologies (ICT) for crisis response and management. Privacy, security and liberty are concepts that have undergone significant changes over time. The authors show how ICT related transformations of sociotechnical practices involved in their enactment create challenges, opportunities and dangers in the context of crisis response. While opportunities include development of more informed, efficient and agile emergency management, dangers include increased surveillance, social sorting, and an erosion of privacy, civil liberties and virtues of humanity. The authors explore causes and mechanisms that underpin these dynamics and measures developed to address them. Against this backdrop, they discuss 'design for privacy' as a socio-technical design approach that empowers people. The aim is to motivate, and explore avenues for, socio-technical innovation that supports information processing and respect for privacy in crisis response and management.

Keywords: Crisis Response, Design for Privacy, Humanity, ICT, Liberty, Privacy, Privacy by Design, Security

INTRODUCTION

A recent stocktaking review of lessons learned from an analysis of international crises as diverse as the Victoria Bush Fires, the London bombings and the 2002 Elbe floods finds that a 'lack of interoperability between first responders and communication problems are the most common findings' (ENISA 2012). Such findings fuel widespread calls for greater interoperability and data sharing, because it seems clear that more interoperability between emergency agencies could enhance societies' capabilities to prepare for and address crises (NATO, 2006, Armstrong, Ashton, & Thomas, 2007; Dawes, Cresswell, & Pardo, 2009; Desourdis & Contestabile, 2011).

At the same time, there has been a 'digital tsunami' – a term coined by an EU Commission 'Future Group' (2007), who observe how individuals, objects and environments generate data through self-disclosure and sensor technology, while advances in data processing make this 'tsunami' of data amenable to analysis for commercial, governance, and security purposes. For crisis management and response, this puts a different mode of command and control within reach, one where more detail

about more factors is available to produce situation awareness more immediately and dynamically, technical interoperability can support information sharing, communication amongst distributed actors and a more broad-based common operational picture, and where computationally augmented detection of patterns can inform sense-making and risk assessment. The fact that populations 'increasingly function as a set of human pantographs, measuring out the world and themselves both at once' has huge potential not only for the emergent 'experimental economy' or 'Lifeworld.Inc' (Thrift, 2011:9), but also for crisis management and response.

However, recent revelations about the extent of such data processing in the name of security (Harding 2014, Rainie, Kiesler, Kang & Madden 2013) have stoked long-standing concerns that there is a dangerous trade-off of privacy and liberty against security:

> *… a new Faustian bargain was struck around 1990. … [In a] 'dance with the digital' … making public through databasing what had been private … many elements of economic and social life are 'locked in' to a path dependent pattern, more of a spider's web than web 2.0. (Urry, 2007:275)*

For Urry, who considers these matters in the context of slow motion crises related to resource shortages (water, soil, oil, finance) and climate change, societies face a choice between all-encompassing surveillance and disastrous chaos as they are 'poised between an Orwellian or Hobbesian future' (ibid: 290). The bargain is Faustian, because choices about these futures are often implicit, folded into everyday life, increasingly hybridizing public and private aspects of life. For example, location and identity information are obtainable even from turned off mobile phones, if telecommunications operators share their data, which they may be obliged to do in disaster situations, where such information may speed up search and rescue, or help contain the spread of infectious diseases (Bengtsson, Lu, Thorson, Garfield & Schreeb, 2011).

However, the idea of an inescapable tradeoff is coming under pressure:

> *We can reach a better balance between privacy and security. We must. There is too much at stake. (Solove, 2011:3)*

Public opinion and policy is changing, demanding more contextual and flexible definitions and approaches and technologies that support respect for people's need for both security and privacy (van Lieshout, Friedewald, Wright, & Gutwirth, 2013; Verfaillie & Van den Herrewegen, 2013). In the European Union especially, there are calls for a position in which security and privacy are not fundamentally opposed, where there is increased individual control (or informational self-determination) of personal data, and rights for the data subject are strengthened (Barnard-Wills, 2013). In this paper we provide an overview of key issues related to security, privacy and liberty and ICT use in crisis response and management to motivate and explore avenues for socio-technical innovation that simultaneously supports information processing for security and respect for privacy and liberty.

WHY DOES IT MATTER? TRANSFORMATIONS OF PRIVACY

In social and political philosophy privacy is often conceptualised as a constitutive element of civil society. Hannah Arendt identifies a separation between public and private as essential for a democratic public realm (1958), because it fosters debate and decisions made on the basis of persuasion and deliberation, not through force and violence. Habermas (1989, 1998), conceives of privacy as a spatial arrangement, practice and value that is crucial for the formation of free subjects able to express themselves and hence capable of participating in public debate. Goffman calls these sheltered spaces of self formation "back region or backstage". It is here where individuals can speak and act freely, relive and rehearse interactions, and try out ideas or positions, for instance in "self talk" (Goffman 1981). And they can do this precisely because they do not have to be conscious or

afraid of 'being watched' and judged. In these conceptions privacy is more than simply something that concerns the individual, it is a functional prerequisite for free democratic societies. Many legal definitions of privacy reflect these concerns and inscribe it into constitutions for democratic societies as the right to be 'let alone' (Brandeis & Warren, 1890). But privacy is necessary not only for civil liberty and democratic freedom. Arendt shows how exclusion, discrimination, humiliation are linked to privacy, extending the concern beyond the role of privacy towards broader concerns with humanity and human rights.

The delicate mechanisms that enable negotiation of public and private separations have been disrupted through the eager appropriation of digital technologies. Over a decade ago, Scott McNealy, then CEO for CISCO, argued that 'You already have zero privacy, get over it' (cited in Langheinrich, 2001). Observations show that citizens behave in contradictory ways in relation to this – on the one hand avowing that privacy and control over personal data are still 'very important' to them (Rainie, Kiesler, Kang, & Madden 2013), on the other seemingly carelessly sharing personal information on a massive scale (Future Group, 2007, Thrift 2011). This suggests a rapidly deepening chasm between theories of and desires for privacy and people's commitment and capacity to translate these into lived practice.

One reason for this is the fact that 'privacy' has many different dimensions: bodily privacy (to protect the integrity of the physical person); territorial privacy (to protect personal space, objects and behaviour); communications privacy (to protect against eavesdropping); locational privacy (to protect against surveillance); and information privacy (to protect personal data) (Santucci 2013, Watson and Finn this issue). Moreover, Helen Nissenbaum (2009) shows that privacy also has multiple meanings depending on context and social norms. While under normal circumstances, most people would not wish their medical data to be available to people other than their doctor, this might change in an emergency, where information about allergies, existing conditions or current medication may be life-saving. In many situations, disclosure of personal information can be delicately modulated.

It is not just a matter of binary bodily or spiritual withdrawal (privacy) or transparency, but a contextual, situated, practically achieved matter of boundary management. Drawing on Irwin Altman's social psychology, Palen and Dourish (2003) distinguish three key boundaries:

- Private/Public: By managing disclosure and giving out only 'enough' information to relevant social groups, a boundary between private and public can be maintained. However, not all disclosure is conscious and not all information can be withheld (e.g. gender, age, movement).
- Identity/Role: Privacy debates often assume that people are primarily concerned about privacy as individuals. However, in most situations, people are social actors and present different aspects of their identity in different social contexts. Emergency responders, for example, act as representatives of institutions. Control over personal data in different roles and role improvisation (Kreps & Bosworth, 1993, Webb, 2004) are critical features of emergency response and involve rationales that differ from those of everyday life. For example, fire fighters may be happy to share intimate physiological data about their breathing with colleagues when entering burning buildings.
- Time/Space: When and where a situation unfolds and how it may be documented for future scrutiny affects people's desire and capacity to control personal information and their expectations.

The capability of information technology to transmit, preserve and capture information changes the nature of these boundaries. Carrying and communicating through digital devices, emergency responders' movements, activities and decisions may be logged and become public through post disaster review committees (e.g. Bech Gjørv 2012) as well as media and social media (Tapia and Lalone this issue). Information from leisure pursuits may spill over into the workplace, and generally

the temporal and spatial 'reach' of information is vastly extended. This creates tension for the control of personal data for both their 'owners' and those processing them, because how information is going to be used in other places, contexts and times cannot always be anticipated. New frontiers for privacy boundary management have emerged, most importantly:

- Movement: Smartphones and social network technologies allow others to see where one is, and mobility patterns can be as uniquely identifying as a finger print (De Montjoye, Hidalgo, Verleysen, & Blondel, 2013). Commercial and intelligence related uses can make informational self determination and selective disclosure virtually impossible (De Souza E Silva & Frith, 2010). For example, US-European counter terrorism collaboration agreements allow US intelligence agencies to examine European air passenger records (Williams, 2012).
- Communication: Whereas the reach of voice and body language in physical spaces – within a command and control room or an airline cockpit – can be modulated to be more or less private, digitally captured traces of such communications are not private.
- Social Networks: The documentation of social connections in social media can be used to personalize services and to profile persons. For example, Google's search engines can be augmented by 'social search' mechanisms (Sherrets, 2008) to leverage information about search patterns and preferences within a person's social network to personalize results. This introduces a need for 'social privacy'.

People have developed sophisticated practices of modulating privacy along these boundaries, but these practices are based on the ability to understand how one person is situated and visible in space, time, and in relation to other individuals, groups or organizations. This is – up to a point – knowable in physical, low-tech, traditional times and spaces, but from the Domesday book commissioned by William the Conqueror in 1086 to record property and personal data for tax and draft purposes to the 10 biggest databases held by agencies like the CIA and organizations like Amazon, Youtube, or Google today1, bureaucratic technologies have engendered a 'steady erosion of clearly situated action' (Grudin 2001, cited in Palen & Dourish, 2003). The proliferation of personal information has given rise to new forms of connected presence (Licoppe, 2004) and comobility (Southern, 2012), and it has altered how we can control the interpretation of our data in different contexts. A number of features play a critical role in this and understanding them better can help us fathom the transformation of privacy more carefully:

- High-Speed Transmission: Data can be sent at very high speeds (up to 26 terabits per second2). • Persistence: It can be stored in large volumes and for long times. • Big Data Analytics: Enhanced computation provides new capabilities of 'qualculation', search, triangulation, actuarial calculations, visualizing data and other forms of computation and enable sophisticated processing of huge data volumes (Thrift, 2004, Kitchin 2014).
- Complexity: Dynamic machine learning and the amount of data processed can make it very difficult, if not impossible for people to understand why certain persons or phenomena are highlighted as 'at risk' or 'of interest'. Some such techniques have been found to be deeply racist or otherwise discriminatory (a reflection or worse, an amplification, of such tendencies within societies) (Introna, 2007). Yet, they 'are beginning to influence every region of life' (Heaven 2013, 35), including security (Bigo, 2009). If crisis management decisions are based on such techniques, decisions are partly made not with but by technologies people do not (and arguably cannot) understand.
- Disembodiment: Processes of data production and access to personal data are disembodied. People often unwittingly generate an 'exhaust' of data (Kitchin 2014), which can be proliferated across different contexts and used in a various ways without the data subjects' being aware of this.
- Dissociation: The results of data processing are often dissociated from the data and the precise actions of selection and analysis that led to them; in other words, people often cannot easily determine who is doing, or did, what, on what basis with their data (Bellotti

and Sellen, 1993). For example, using publicly available data from many sources, commercial service providers like Hirecheck can facilitate employment decisions (Solove, 2004), while use of data from social services can help the UK fire service identify individuals at risk to provide them with education and support (Knight, 2013), potentially resulting in inscrutably Kafkaesque exclusions or disciplinary attentions (Solove 2004).

- Addressability: A range of generalized and standardized grids and metrics, combined with the proliferation of data, make people and objects increasingly locatable, creating 'a global architecture of address', where 'each and every part of the world could in theory be given an address' (Thrift, 2007:94, see also Crang and Graham, 2007, Graham, 2009).

For crisis management these are powerful and useful affordances.

OPPORTUNITIES, CHALLENGES AND DANGERS

Opportunities, challenges and dangers are rarely clear-cut, and they are not separate aspects of either social or technical dimensions of innovation. Many emergency responders and managers invest high hopes in technology 'that provides the right information, at the right time, and in the right place', because they share the belief that it

> *…has the potential to reduce disaster impacts. It enables managers to plan more effectively for a wide range of hazards and to react more quickly and effectively when the unexpected inevitably happens. (Koua, MacEachren, Turtun, Pezanowski, Tomaszewski, & Frazier, 2010:255)*

There is significant evidence that suggests that matters are more complex than just making more information available (Heath & Luff, 1992; Bannon & Bødker 1997; Wolbers & Boersma 2013), but also some truth in this. But working with information is difficult. Numerous post-disaster reviews of multi-agency emergency response highlight failure to share data as a serious challenge. Reflecting on evaluations of the emergency response effort after the London 7/7 bombings in 2005, Hilary Armstrong, UK Cabinet Minister for Social Exclusion, pointed out that:

> *It was apparent that in some parts of the emergency response, the requirements of the Data Protection Act 1998 were either misinterpreted or over-zealously applied. Subsequent reports … have indicated that the London experience in this respect is not unique. (Armstrong, Ashton & Thomas, 2007)*

In the aftermath of the London bombings, data controllers considered that it was not legal to pass personal data initially collected from victims by the Family Assistance Centre on to successor organizations for follow-up support. This complicated continuity of care for people and led to a fragmentation of response efforts. 'Silo-thinking', or a lack of organizational interoperability, where individual agencies do not collaborate even where this would be useful and possible is widely seen as one of the main barriers to organisational interaction (Dawes 2009, Cole 2010, Desourdis 2012). Technology is often seen as a solution. After the 2011 Norway attacks, for example, the specially appointed expert committee concluded that

> *The authorities' ability to protect the people on Utøya Island failed. A more rapid police operation was a realistic possibility.*

And they identified that a key reason for such failure was the fact that 'the potential inherent in information and communications technology has not been exploited well enough' (Bech Gjørv, 2012:Part IV).

As a result of such critiques of social, organizational and technical challenges, systems of systems approaches that envisage flexible assembly and coordination of relevant services, organizations,

information sources and resources at system runtime are gaining ground. In the US Department of Homeland Security's definition:

> *A system of systems exists when a group of independently operating systems—comprised of people, technology, and organizations—are connected, enabling emergency responders to effectively support day-to-day operations, planned events, or major incidents. (US Dept. for Homeland Security, 2004: 1)*

One particularly striking instantiation of system of systems visions is a project where NCOIC – the Network Centric Operations Industry Consortium – brought together major industry players like Boeing, defence technology suppliers, government and non-government emergency response agencies, and IT firms, who invested 1.2 million dollars in integrating their services and information systems. In 2013, this culminated in a Geospatial Community Cloud Concept Demonstration, with the group re-enacting the international response to the Haiti earthquake over a whole day. There are numerous videos that propose that overall, this could massively enhance the efficiency of emergency response[3].

As Ellebrecht and Kaufman (in this issue) show, a straight-forward translation into efficiency gains is questionable. Often advantages of socio-technical innovation are more complex, and require more than a new technology, and come with positive and negative unintended consequences that are impossible to predict. While such complexities and uncertainties are often acknowledged, the focus frequently remains firmly on the pursuit of efficiency through technology. In the European context, where the emphasis is strongly on 'unity in diversity', the centralization and standardization efforts complemented with a subsidiarity principle of devolving decision-making to the lowest possible level (whilst supporting coordinative action at a higher level). This echoes US researchers' call for support for the situated assembly of appropriate 'adhocracies' and improvisation, and a focus on 'emergent interoperability' (Mendonça, Jefferson, & Harrald, 2007).

Ideas of emergent interoperability, that is, an ability to connect systems on the fly, based on standard protocols and/or mechanisms of virtualization, wrapping and translation, open up new capabilities to enhance security for citizens through more flexible use of data. New forms of interoperability can enable more 'agile response' (Harrald, 2006), that is, more richly and dynamically informed collaboration. The concept of agile response describes a flexible, loosely coupled, but highly collaborative response effort, where people have a high and highly distributed real-time degree of awareness of activities and resources and are able to mobilize these effectively in a coordinated manner. The concept resonates with visions of 'smart cities' that enable integration of different services, from healthcare to transport management, to insurance, taxation and e-government. Although some nations – especially countries like Germany and Romania, who have experienced totalitarian regimes, oppose such moves (Barnard-Wills, 2013), there are a number of examples worldwide where integration across civil, commercial and public safety services is gaining ground. Rio De Janeiro, for example, facilitates collaboration between routine transportation management and crisis management (Naphade, Banavar, Harrison, Paraszczak, & Morris, 2011). Other countries, like Japan, are implementing visions of 'the future resilient society' through integration of personal data across municipal, commercial, executive and juridical fields of everyday life and crisis management (Maeda, 2010) (Figure 1).

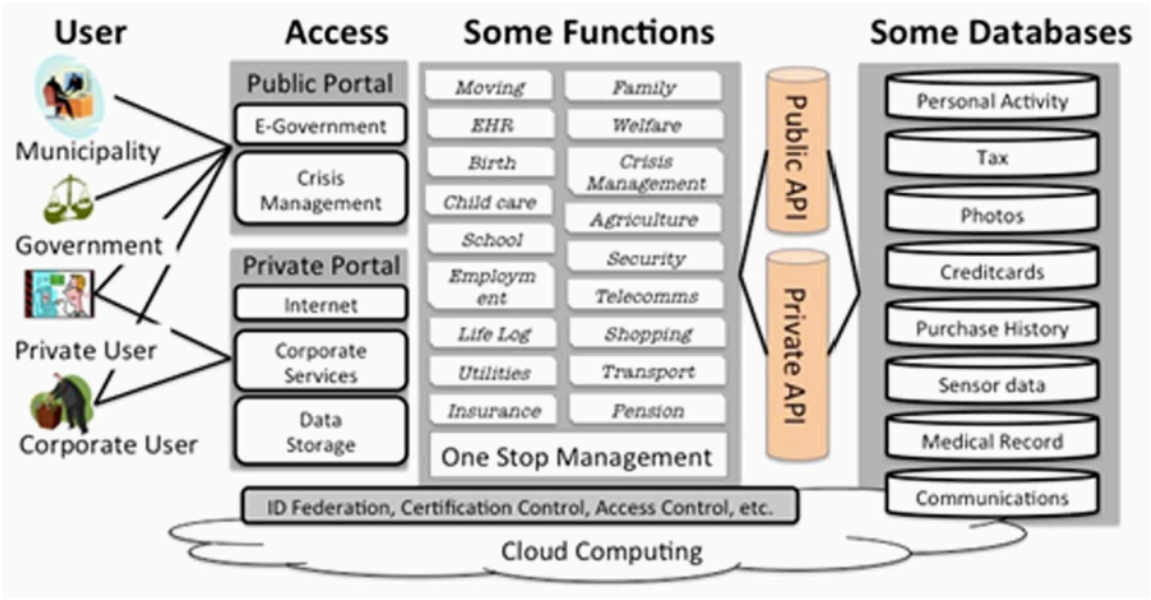

Figure 1. 'Next generation ICT services for the resilient society' (adapted from Maeda 2010)

While such interoperability could be powerful for beneficial purposes, the digital tsunami it rides on can also foster the development of a technological and bureaucratic apparatus for all encompassing surveillance. The latter is not an inevitable consequence of pursuing the former, but to explore avenues for design, it is important to discuss key dangers in some depth.

SURVEILLANCE, SOCIAL SORTING, AND AN EROSION OF CIVIL LIBERTIES

Recent debates about 'Safeguarding Privacy in a connected world' (European Commission, 2012) highlight citizen's fears over surveillance. They show that current privacy protection is flawed, undermining well-meant efforts to utilise intelligence to enhance efficiency and security within European societies as well as giving rise to an excess of surveillance. New data protection regulations are being drawn up to take account of technological advances and to address key issues in the processing of personal data, particularly conditions of consent, transparency, data access for data subjects, rights to rectification and erasure, the right to object and the right not to be subject to profiling, obligations of data controllers, and exceptions to the fundamental right to personal data protection (European Commission, 2012).

It is critical for designers of ICT for crisis response and management to address these issues. If regulators, citizens or professionals are worried about privacy, they will not (allow) use of new technologies even if they could enhance the efficiency of emergency services. Perhaps Figure 1. 'Next generation ICT services for the resilient society' (adapted from Maeda 2010) even more worryingly, technologies may be used in ways that extend surveillance in ways that undermine civil liberties and freedoms. The dynamics of such unintended consequences are not easy to circumscribe, they are often hidden and multi-causal. This section explores some of the most important issues, ranging from surveillance to exclusionary discipline, false positives, social sorting, liability, cultures of fear, and a militarization of emergency response.

Sherry Turkle (2011) shows that we live 'a life that generates its own electronic shadow' (p. 260). However, particularly for those who have grown up in new regimes of surveillance that today characterize many societies and economies, leaving an electronic trace can come to feel so natural that the shadow seems to disappear. This naturalized, invisible regime of surveillance has corrosive potential. Michel Foucault, a historian and philosopher who explored technologically augmented disciplinary rationalities, shows how individuals whose private lives may be scrutinized by authorities are likely to internalize control into their very body and soul (Foucault, 1977). Foucault makes an

important distinction between inclusionary and exclusionary discipline that is helpful for analysing and designing ICT for crisis response and management. He observes the emergence of inclusionary discipline during the 17th Century plague pandemic, an important point of origin for innovation in personal data processing. New forms of census registered people in their homes, recorded their name and health status. This allowed the authorities to know about deaths, to collect and remove the dead and to train people to deal with the disease. In the process, 'docile' citizens emerged that would subject themselves, if not willingly, then mostly quietly to surveillance and crisis management measures. This was inclusionary, because those subject to surveillance remained inside society and became part of the management of the crisis. The treatment of leprosy – a more creeping crisis – was very different. It implied identification of those infected, then separation and often permanent exile from society, a form of exclusionary discipline.

The exclusionary power of digital profiling techniques is – for some analysts today – of even greater concern than the erosion of privacy. They are 'less worried about privacy and more worried about the abuse of probabilistic prediction' (Mayer-Schönberger, in Heaven 2013, 35), because they can be based on processes that are alien to human reasoning. Moreover, exclusion, especially when based on inscrutable analysis of personal data, can lead to a 'splintering' of societies and undermine societal virtues of humanity, equality, solidarity and fairness (Graham & Marvin, 2001).

Clive Norris' analysis (2002) maps Foucault's analysis onto a discussion of digital surveillance and an exclusionary digital disciplinary society. He shows how powerful 'next generation' ICT are able to combine, for example, CCTV, facial recognition analytics, automatic number plate recognition (ANPR) and policing databases. Individuals may be subject to surreptitious capture of personal data, for example through face recognition and behavioural biometrics. A critical danger here is that individuals may become 'false positives', that is, falsely identified as a target for action (or refusal of service). This is a particularly strong risk during and after emergency situations. For example, in their investigations into a thwarted bombing attack shortly after the 2005 7/7 London bombings, the UK police incorrectly identified Jean Charles de Menezes as Hussain Osman, one of the organisers of the attack. This eventually led to Mr de Menezes being shot dead. More broadly, particular groups within society may be discriminated against due to technologically augmented capabilities to carry out 'social sorting', that is, categorization based on criteria such as ethnicity, economic status, age, gender, health status but also more flexible 'markers' across different data sets. For example, in 2009 in the UK, 'protester' markers were accumulated and connected to vehicles and their owners which were then entered into national ANPR-based transport monitoring systems, which led to peaceful protesters being searched and obstructed. This endangers freedoms of association and also constitutes an instance of 'function creep', that is, the reuse of data collected for one purpose for another, unrelated purpose.

When combined with exceptions to normal data protection rules that apply under conditions of emergency, these new technologies can open new doors for repurposing personal data. Actuarial analytics that originate from the insurance sector have, for example, been introduced to policing (Feeley and Simon, 1994), where they have 'become at least as important as reactive penal measures' (Zedner, 2007: 265). Actuarial analysis is problematic, because it allows social sorting and categorical exclusion, that is, exclusion not based on individual history but on the fact that one belongs to a certain category of persons who are deemed 'suspicious' or 'undeserving'. It 'eschews corrective aspirations, takes crime and deviance for granted, and seeks technical means and measures to manage the threat they represent' (Yar, 2003: 256). Austerity and increased occurrence of crises that stretch response capacity exert pressure to utilize such preventative, actuarial, exclusionary measures. Solove (2004) argues that in the light of such techniques, traditional metaphors of surveillance (such as Big Brother) could usefully be elaborated through Kafka's novel The Trial (Kafka, 2000), a novel that chronicles feelings of exclusion, helplessness and frustration in relation to disembodied, dissociated surveillance and profiling, done with unclear accountability and little control on the individual's part over the gathering, processing and storing of data.

Automated data analysis has the potential to be particularly pernicious. It draws on data collected from different sources which may contain missing or obsolete data. If data cleaning is not conducted properly, mistakes – e.g. false positives – can occur. At this juncture, arguments that assume that 'if you have nothing to hide, you need not worry about surveillance', really crumble. With a false positive rate of 1%, which is as low as statistical inference can normally be, the American Computer Assisted Passenger Prescreening System might scrutinize the 1.8 million that travel by air in the US and mark 18,000 innocent people as suspects every day (Solove, 2008). The consequences may not be dramatic or even fatal as they were for Jean Charles de Menezes and his family, but they can be serious. On the other hand, processing might not accurately distinguish noise from important information, leading to false negatives, that is, failing to identify relevant instances (such as a trapped victim or a criminal). The use of automated data analysis also undermines values of equality, solidarity and humanity by institutionalising machine recognisable indicators and judgement based on stereotypes.

The new temporality of privacy creates further tensions. The default when designing ICT for emergency management is to keep records as detailed and as lasting as possible, including records of actions and decisions taken by emergency response professionals and experts. This thinking complicates embodied control of personal information and privacy management (Bannon, 2006; Dodge & Kitchin, 2007). The unforgetting accumulation of data can, for example, allow inappropriate retrospective scrutiny of decisions and actions. The verdict in the l'Aquila trial in 2012, where six scientists and an official of Italy's Civil Protection Agency were convicted of manslaughter for providing false reassurances to the public regarding the earthquake, is an extreme example of how the ability of tracking who said what and when may affect the retrospective accountability of emergency responders.

As we have already raised, for societies, the collection and processing of personal data may become problematic because basic human rights, such as freedoms of speech, association and movement and human values can be eroded. Further to this, contemporary constructions of risk and danger, especially since the start of the 'war on terror' after 9/11, may be leading societies into a permanent state of emergency/ exception. A potent driver is the transformation of fear, which, according to sociologist Frank Furedi: 'is no longer simply an emotion, or a response to the perception of threat. It has become a cultural idiom …. Popular culture continually encourages an expansive alarmist imagination' (Furedi, 2006). Fearful societies have begun to accept, or even call for, a farreaching securitization, even 'militarization of everyday life' (Graham, 2010), that is, an embedding of security/military perspectives and technologies into everyday spaces and everyday lives, from all-surround CCTV to the use of blast proof concrete in buildings. ICT for crisis response and management, too, are embracing military inspired technologies, such as the incident command system (ICS) structures, GPS, robots and unmanned aerial vehicles (UAV) or drones. The embedding of military technologies into everyday life and ICT has a long history, from the Internet to GPS. However, recent years have seen an acceleration, as technology companies bound up with the military – seeing military budgets shrink – begin to sell to civilian and public authority users, and create new products that are no longer purely military or purely civilian (Murakami Wood, Ball, Lyon, Norris, & Raab, 2006). This doubling, or re-orientation and integration of military metaphors and technologies into emergency response is a delicate enterprise. They can detrimentally affect the way in which emergency management is done: The centralization of emergency response under the Department of Homeland Security in the US after 9/11, for example, played a significant part in the failure of humanitarian response to Katrina. Adoption of military based hierarchical organisation principles and a focus on protection from malicious attacks weakened data protection, strengthened command and control approaches and eased activation of police and military. Research suggests that this top down approach diminished the emergency services' capability to activate community resilience and respond to natural disasters. It shifted attention from mitigation to response, placed 'homeland security threats higher on the agenda than preparation for regular, but catastrophic, natural disasters' and hampered locally flexible emergency management (Birkland, 2009: 430, see

also Tierney, 2006)). The response to Katrina was, for example, 'marred by coordination failures, as most participants … reportedly were unaware of the exact workings of ICS' (Ansell, Boin, & Keller, 2010: 203, see also Haddow & Bullock, 2005).

A militarization of emergency response and everyday culture also contributes to what Giorgio Agamben (2005) describes as a spread of exceptions, often declared to protect national security. European history is marked by the devastating experience of two world wars and the holocaust, which were facilitated by an unprecedentedly effective process of collecting, sharing and processing personal data through a bureaucratic apparatus and culture of surveillance (Arendt, 2004; Bauman, 1989). Totalitarian rule was established in part through the evocation of extra-legal 'states of exception', which suspended fundamental human rights and data protection laws, because it was assumed that 'the rule of law may prevent a [state] from defending itself' (Scheppele, 2003: 1010). This experience demonstrates that a softening of separations between data controllers can have severe consequences for societies. These experiences colour much of the political response to the 'war on terror':

> *…much of the international community … has turned away from these extra-legal justifications for states of exception. … Only the United States, with its eighteenth century constitution and Cold War legacy of exceptionalism, seems to be soldiering on in this new legal space of conflict (Scheppele 2003: 1082)*

But US philosophies of extra-legal exceptionalism, where the power to define exceptions is concentrated in the hands of individuals, are highly influential when it comes to the design of information systems of systems with permeable boundaries between data controllers, persistent storage, and powerful analytic and visualizing capacities. The convergence between crisis ICT and smart city systems and their supporting architectures, are examples. A key issue here is the removal of boundaries that separate criminal investigations from national security investigations. For example, in the UK calls for 'smart city' convergence between Transport for London and police systems, and the extension of the ANPR system's use from congestion charging to policing related to national security as well as investigations for general criminal policing echo controversies around the US Patriot Act, aimed at 'Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism'. The Act was passed in 2001, and it enables extensive processing of personal data, including records of commercial transactions and Passenger Name Records collected in third countries, such as European member states (Whittaker, 2011).

A TRANSFORMATION OF PRIVACY

The dangers we have outlined in the previous section are, in part, allowed to coalesce and undermine the benign potential of socio-technical innovation, because design has failed to support citizens to 'feel' the intrusion into their privacy. Pre-emptive measures are often localised, unplanned, enabled by invisible infrastructure and powered by blackboxed interoperability between systems (Amoore, 2011). Genuine and imagined threats and economic pressures on the provision of emergency services seem to require the maximization of data sharing. Thus the advance of surveillance is creeping, disembodied, invisible and passive, and rationalized by hopeful discourses of enhanced efficiency on the one hand, and fearful discourses of security on the other. How could IT be designed differently?

Many of the new technological capabilities are problematic, because they fail to support and even obstruct lived practices of privacy boundary management. In pre-digital environments, people can modulate the disclosure of personal information dependent on context, controlling it through embodied conduct embedded in material environments, through providing or withholding information in relations with other people but also with governments, bureaucracies and official and commercial organizations such as healthcare providers, local authorities, or telecommunications operators, through agreements with data controllers, and through freedom of information requests

about the data that is held about one's person. Our account of opportunities, challenges and dangers suggests some opportunities for intervention through circumspect design and innovative appropriation of ICT into crisis response and management exist, which we will now consider briefly. These opportunities arise around efforts to enhance people's abilities to:

- Notice instances of data production, collection, and generally processing
- Know who is looking and why
- Comprehend digitally augmented, dynamically changing spatial, temporal, social and political contexts,
- Negotiate and agree proportionate and appropriate practices
- Notice that such agreements are adhered to and, if necessary, enforce them or be able to demand enforcement

To support the practices involved in this, design of crisis response and management technologies needs to shift the focus from merely regulating and monitoring 'access' to personal data to supporting diverse stakeholders in managing privacy boundaries – emergency responders, public authorities, the individuals and communities affected by disasters, as well as members of the general public. Such support should also allow people to notice potentially complex value conflicts, to determine and negotiate the proportionality and legitimacy of data processing, to actively trust (or withdraw trust) from data controllers and agree a level of granularity of personal data that is appropriate to the situation. A number of approaches exist, including privacy by design, privacy preserving techniques and privacy enhancing technologies (Fischer-Hübner, Hoofnagle, Krontiris, Rannenberg & Waidner, 2011).

DESIGNING FOR PRIVACY

Privacy sensitive agile emergency response supported by technologies that also allow people to notice and address unintended consequences and wider societal impact is a hopeful vision. Realizing it is a challenging balancing act for design. In this section we seek to contribute to larger efforts of addressing challenges, by discussing 'design for privacy' as a particularly promising avenue for innovation.

Privacy by design is a relatively new approach and it has several meanings and origins (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 that allow people to maintain a degree of anonymity (Pearson, 2009). Both approaches need to be supplemented with methods that support translation into the design and appropriation of technologies. Such methodologies may include privacy and ethical impact assessments, that is, structured investigations into the privacy and ethical implications of design decisions (Clarke, 2009; Wright, 2010), and legal risk analysis. All should "begin at the earliest possible stages, when there are still opportunities to influence the outcome of a project" (Wright & De Heert, 2012). In our own work, we combine privacy and ethical impact assessment with more qualitative ethnographic and participatory design approaches that explore privacy and ethical issues through observation, collaborative design and iterative experimental implementation (Ramirez and Buscher, 2012). This is motivated by the contextual, practiced nature of privacy boundary management, which requires that designers understand and anticipate how technologies might be used effectively as an integral part of such (changing) practices.

This approach has shown that inscribing compliance into technologies, e.g. through privacy by design approaches can be of limited utility in view of the dynamic nature of emergency management and the need for role improvisation and emergent interoperability in systems of systems approaches. Privacy cannot easily usefully be ensured or 'enforced' apriori by design in this context.

However, our qualitative studies and experimental engagement with stakeholders have also highlighted a third approach of human-practice focused privacy by design. This is based on a shift from conceptions of privacy as a value that has to be traded in in return for security, or a right that has to be respected through regulation, to an understanding of privacy as a contextual, situated and embodied practice of boundary management that is augmented and constrained by technologies, cultural conventions and the law. By taking this perspective, alternative socio-technical design avenues are opened up, for example via specification of non-functional requirements such as architectural qualities of transparency and inspectability. For example, privacy protection in emergency response systems of systems may be supported by imposing temporal and geographical constraints on data sharing, 'seamful design' (Chalmers, 2003) and approaches that support 'accountable' or 'palpable' computing (Dourish, 2001, Kyng, 2007).

When, in times of crises, boundaries between different systems (telecoms databases, transport management systems, police records, social networking systems, insurance databases) are made permeable, allowing automated data collection, data mining, analysis and profiling, conventional privacy protection that involves limiting access at the point of data collection, including using legal, cryptographic and statistical techniques is likely to be prohibitively rigid and restrictive. Accountable datamining, an approach developed in response to the fact that the Internet provides a huge source of data that can render conventional access-limiting methods ineffective and impractical, is an example of innovative privacy solutions that may be useful in a human practice focused approach. Referring to the US use of data mining around Passenger Records, Weitzner, Abelson, Berners-Lee, Feigenbaum, Hendler & Sussman, (2008:85) argue that: 'Laws that limit access to information do not protect privacy here because so much of the data is publicly available. To date, neither law nor technology has developed a way to address this privacy loophole.' New socio-technical mechanisms are required and Weitzner and his colleagues suggest:

- Transparency: Mechanisms where the history of data manipulations and inferences is maintained and can be examined by authorized parties (who may be the general public)
- Accountability: One can check whether policies that govern data processing were in fact adhered to (Weitzner, Abelson, Berners-Lee, Hanson, Hendler, Kagal, McGuiness, Sussman & Waterman, 2006:)

In the context of emergency response exceptional breaches of data protection regulations may be necessary and legitimate. Personal data may, for example, be used for purposes other than those specified at the time of collection. To support trust in systems that support interoperability in times of crisis (but not under normal circumstances), the design of tools that make the use of personal data accountable both at the time of use and retrospectively, seems promising. Our research also suggests that in view of the substantive ethical and legal challenges, a human practice focused co-design approach is particularly useful for crisis ICT design, because it brings in located accountabilities (Suchman, 2002) and enables collective, iterative development of understanding of challenges and search for socio-technical solutions.

CONCLUSION

The main contribution of this paper is a discussion of key opportunities, challenges and dangers of utilizing personal data through ICT in crisis response and management. We argue that there has been a transformation of privacy and what privacy means and how it can be practiced is changing significantly, whilst current technologies do not support the practices required for privacy management adequately, especially not in the context of crisis response and management. It is important to translate enhanced privacy sensitivity into design, and we have highlighted limitations of approaches that seek to inscribe compliance into technologies and recommended and alternative approach of designing for privacy as a promising avenue for design. Our investigation suggests that while compliance with values of privacy can, in some instances, be designed 'into' technology, in the dynamic context of crisis management, where flexibility is needed with regard to what kinds of

information sources can be used and how, an approach that seeks to design for privacy in the sense of supporting accountability amongst the technologies, the professional responders as well as other stakeholders and the public in noticing, negotiating and managing privacy is a more effective and useful approach.

ACKNOWLEDGMENT

We would like to thank our anonymous ISCRAM reviewers, and our colleagues in the Centre for Mobilities Research, Lancaster University, the BRIDGE project, and the SecInCore project, especially Lucas Introna, Peter Wahlgren, Matts Ahlsen, Bernard Van Veelen, and Leonardo Ramirez for discussions on privacy. The work presented is part of research funded by the European Union 7th Framework Programme in the BRIDGE project (Grant no: 261817) and SecInCoRe project (Grant no: 261817).

REFERENCES

Agamben, G. (2005). *State of Exception*. Chicago: Chicago University Press.

Altman, I. (1976). Privacy: A Conceptual Analysis. *Environment and Behavior*, 8(1), 7–29.

Amoore, L. (2011). Data Derivatives: On the Emergence of a Security Risk Calculus for Our Times. *Theory, Culture & Society*, 28(6), 24–43. doi:10.1177/0263276411417430

Andersen, P. (2007). PalCom: Palpable Computing Open architecture. Aarhus. Retrieved from http:// www.istpalcom.org/publications/deliverables/ Deliverable-54-[2.2.3]-open-architecture.pdf

Arendt, H. (1958) *The Human Condition*. Chicago: University of Chicago Press. Arendt, H. (2004). The Origins of Totalitarianism. New York: Harvest Books.

Armstrong, H., Ashton, C., & Thomas, R. (2007). Data Protection and Sharing – Guidance for Emergency Planners and Responders. London. www.cabinetoffice.gov.uk/media/132709/dataprotection.pdf

Bannon, L. (2006). Forgetting as a Feature, Not a Bug: The Duality of Memory and Implications for Ubiquitous Computing. *CoDesign*, 2(1), 3–15. doi:10.1080/15710880600608230

Bannon, L., & Bødker, S. (1997). Constructing Common Information Spaces. In *Proceedings of the Fifth European Conference on Computer Supported Cooperative Work* 1997:81-96. doi:10.1007/978-94- 015-7372-6_6

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

Bauman, Z. (1989). *Modernity and the Holocaust*. Contemporary Sociology, 20, 267.

Bech Gjørv, A. (2012). Rapport fra 22 Juli-Kommisjonen. Oslo. Retrieved from http://www.regjeringen. no/smk/html/22julikommisjonen/22JULIKOMMISJ ONEN_NO/INDEX.HTM [Accessed 13 July 2014]

Bengtsson, L., Lu, X., Thorson, A., Garfield, R., & Schreeb, J. (2011). Improved Response to Disasters and Outbreaks by Tracking Population Movements with Mobile Phone Network Data: A Post-Earthquake Geospatial Study in Haiti. PLoS Medicine, 8(8), e1001083. doi:10.1371/journal.pmed.1001083 PMID:21918643

Bigo, D. (2009) The Future Perfect of (In)security (P8): Pre-crime Strategy, Proactivity, Pre-emption, Prevention, Precaution, Profiling, Prediction and Privacy. Paper presented at the Institute for Hazard and Risk Research, Durham University, November. http:// www.interdisciplines.org/paper.php?paperID=342

Birkland, T. A. (2009). Disasters, Catastrophes, and Policy Failure in the Homeland Security Era. *Review of Policy Research*, 26(4), 423–438. doi:10.1111/ j.1541-1338.2009.00393.x Brandeis, L. D., & Warren, S. D. (1890). The Right to Privacy. Harvard Law Review, IV, 193–220.

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]

Chalmers, M. (2003). Seamful design and ubicomp infrastructure. *Proceedings of Ubicomp Workshop at the Crossroads The Interaction of HCI and Systems Issues in UbiComp*. http://www.dcs.gla. ac.uk/~matthew/papers/ubicomp2003HCISystems. pdf [Accessed 29 September 2014]

Clarke, R. (2009). Privacy Impact Assessment: Its Origins and Development. *Computer Law & Security Report*, 25(2), 123–135. doi:10.1016/j. clsr.2009.02.002

Cole, J. (2010). Interoperability in a Crisis. Human Factors and Organisational Processes. http://www.rusi.org/downloads/assets/Interoperability_2_web. pdf [Accessed 22 Nov 2012]

Crang, M., & Graham, S. (2007). Sentient Cities: Ambient Intelligence and the Politics of Urban Apace. *Information Communication and Society*, 10(6), 789–817. doi:10.1080/13691180701750991

De Souza, E., Silva, A., & Frith, J. (2010). Locational Privacy in Public Spaces: Media Discourses on Location-Aware Mobile Technologies. *Communication, Culture & Critique*, 3(4), 503–525. doi:10.1111/j.1753-9137.2010.01083.x

Dodge, M., & Kitchin, R. (2007). Outlines of a World Coming into Existence: Pervasive Computing and the Ethics of Forgetting. *Environment and Planning. B, Planning & Design*, 34(3), 431–445. doi:10.1068/b32041t

Dourish, P. (2001). *Where the action is.* Cambridge, MA: MIT Press.

European Commission. (2012). Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) (Vol. 11). http://ec.europa. eu/justice/data-protection/document/review2012/ com_2012_11_en.pdf [Accessed 25 Nov 2012]

European Commission. (2012). Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century. Brussels.

European Union Agency for Network and Information Security (ENISA). (2012). Emergency Communications Stocktaking. A study into Emergency Communications Procedures. Retrieved from http:// www.enisa.europa.eu/media/news-items/reportlooks- at-improving-emergency-communications [Accessed 12 July 2014]

Fischer-Hübner, S., Hoofnagle, C., Krontiris, I., Rannenberg, K., & Waidner, M. (2011). Online Privacy: Towards Informational Self-Determination on the Internet *Online*, 1(1), 1–20.

Foucault, M. (1995). *Discipline and Punish*. New York: Random House. (Original work published 1977)

Furedi, F. (2006). *Culture of Fear*. Continuum International Publishing Group Ltd.

Future Group. (2007). Public Security, Privacy and Technology in Europe: Moving Forward. http://www. statewatch.org/news/2008/jul/eu-futures-dec-secprivacy- 2007.pdf [Accessed 25 Nov 2012]

Goffman, E. (1981). *Forms of Talk*. Philadelphia: University of Pennsylvania Press.

Graham, S. (2008). *Cities Under Siege: The New Military Urbanism*. London: Verso.

Graham, S., & Marvin, S. (2001). *Splintering urbanism*. London: Routledge.

Habermas, J. (1989). *The Structural transformation of the public sphere* (T. Berger & F. Lawrence, Trans.). Cambridge, Mass.: MIT Press.

Habermas, J. (1998). *Between Facts and Norms: Contributors to a Discourse Theory of Law and Democracy* (W. Rehg, Trans.). Cambridge: MIT Press.

Harding, L. (2014). *The Snowden Files: The Inside Story of the World's Most Wanted Man*. London: Guardian Faber Publishing.

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. doi:10.1177/0002716205285404

Heath, C., & Luff, P. (1992). Collaboration and Control: Crisis management and multimedia technology in London Underground Line Control Rooms. *Computer Supported Cooperative Work*, 1(1-2), 69–94. doi:10.1007/BF00752451

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. doi:10.1007/s10676-006-9133-z

Kafka, F. (2000). *The Trial*. London: Penguin Classics.

Knight, K. (2013). Facing the future. Findings from the Review of Efficiencies and Operations in Fire and Rescue Authorities in England. Her Majesty's Stationery Office. https://www.gov.uk/government/ publications/facing-the-future [Accessed 29 September 2014]

Koua, E. L., MacEachren, A. M., Turtun, I., Pezanowski, S., Tomaszewski, B., & Frazier, T. (2010). Conceotualizing 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.

Kreps, G. A., & Bosworth, S. L. (1993). Disaster, Organizing and Role Enactment: A Structural Approach. *American Journal of Sociology*, 99(2), 428–463. doi:10.1086/230270

Kyng, M. (2007) (Ed.). Revised Conceptual Framework for Palpable Computing. http://www.ist-palcom. org/publications/deliverables/Deliverable-37- [2.1.2]-palpability-revised-SectionI.pdf [Accessed 29 September 2014]

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

Licoppe, C. (2004). "Connected" presence: The Emergence of a New Repertoire for Managing Social Relationships in a Changing Communication Technoscape. *Environment and Planning. D, Society & Space*, 22(1), 135–156. doi:10.1068/d323t

Maeda, Y., Higashida, M., Iwatsuki, K., Handa, T., Kihara, Y., & Hayashi, H. (2010a). Next Generation ICT Services Underlying the Resilient Society. *Journal of Disaster Research*, 5(6), 627–635.

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), 44–49. doi:10.1145/1226736.1226764

Murakami Wood, D., Ball, K., Lyon, D., Norris, C., & Raab, C. (2006). A Report on the Surveillance Society - For the Information Commissioner by the Surveillance Studies Network. http://ico.org. uk/~/media/documents/library/Data_Protection/ Practical_application/SURVEILLANCE_SOCIETY_ FULL_REPORT_2006.PDF [Accessed 27 September 2014]

Naphade, M., Banavar, G., Harrison, C., Paraszczak, J., & Morris, R. (2011). Smarter Cities and Their Innovation Challenges. *Computer*, 44(6), 32–39. doi:10.1109/MC.2011.187

Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford University Press.

Norris, C. (2002). From Personal to Digital: CCTV, the Panopticon, and the Technological Mediation of Suspicion and Social Control. (pp. 249-281) In D. Lyon (Ed.), *Surveillance as Social Sorting*. Routledge.

Palen, L., & Dourish, P. (2003). Unpacking "Privacy" for a Networked World. *Proceedings of the conference on Human factors in computing systems CHI 03*, 5(5), 129-136. ACM Press. doi:10.1145/642611.642635

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

Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013). Anonymity, Privacy, and Security Online | Pew Research Center's Internet & American Life Project. Pew Research Internet Project. http://www. pewinternet.org/2013/09/05/anonymity-privacyand- security-online/ [Accessed 12 July 2014]

Ramirez, L., & Buscher, M. (2012). Domain Analysis - Interoperability and Integration. Bridge Project Deliverable D2.2. Available from the authors

Solove, D. J. (2004). *The Digital Person: Technology and Privacy in the Information Age*. NY: NYU Press.

Solove, D. J. (2008). Data Mining and the Security- Liberty Debate. [SSRN.]. *The University of Chicago Law Review. University of Chicago. Law School*, 75(1), 66–67.

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

Southern, J. (2012). Comobility: How Proximity and Distance Travel Together in Locative Media. *Canadian Journal of Communication*, 37(1), 75–91.

Suchman, L. (2002). Located accountabilities in technology production. *Scandinavian Journal of Information Systems* - Special Issue on Ethnography and Intervention Archive, 14(2), 91–105.

Thrift, N. (2004). Movement-space: The Changing Domain of Thinking Resulting from the Development of New Kinds of Spatial Awareness. *Economy and Society,* 33(4), 582–604. doi:10.1080/0308514042000285305

Thrift, N. (2007). Non-representational Theory: Space, Politics, Affect. London: Routledge. 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

Tierney, K. (2006). Metaphors Matter: Disaster Myths, Media Frames, and Their Consequences in Hurricane Katrina. *The Annals of the American Academy of Political and Social Science*, 604(1), 57–81. doi:10.1177/0002716205285589

Turkle, S. (2011). *Alone Together*. New York: Basic Books.

Urry, J. (2007). *Mobilities*. Cambridge: Polity.

US Department of Homeland Security. (2004). The System of Systems Approach for Interoperable Communications. http://www.npstc.org/download. jsp?tableId=37&column=217&id=2458&file=SOS ApproachforInteroperableCommunications_02.pdf [Accessed 27 September 2014].

Van De Walle, B., Turoff, M., & Hiltz, S. R. (2010). *Information Systems for Emergency Management*. Armonk, NY: M.E.Sharpe.

Webb, G. R. (2004). Role Improvising during Crisis Situations. *International Journal of Emergency Management*, 2(1/2), 47–61. doi:10.1504/ IJEM.2004.005230

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. doi:10.1145/1349026.1349043

Weitzner, D. J., Abelson, H., Hanson, C., Hendler, J., Kagal, L., McGuinness, D. L., (2006). Transparent Accountable Data Mining: New Strategies for Privacy Protection. Artificial Intelligence. MIT CSAIL Technical Report-2006-007. http://www. w3.org/2006/01/tami-privacy-strategies-aaai.pdf [Accessed 27 September 2014].

Whittaker, Z. (2011). Summary: USA PATRIOT Act series. ZDNet. http://www.zdnet.com/blog/igeneration/ summary-zdnets-usa-patriot-act-series/9233 [Accessed 27 September 2014].

Wolbers, J., & Boersma, K. (2013). The Common Operational Picture as Collective Sensemaking. *Journal of Contingencies and Crisis Management*, 21(4), 186–199. doi:10.1111/1468-5973.12027

Wright, D. (2010). 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

Wright, D., & DeHeert, P. (2012). *Privacy Impact Assessment*. Springer Netherlands. doi:10.1007/978- 94-007-2543-0

ENDNOTES

1 http://www.comparebusinessproducts.com/ fyi/10-largest-databases-in-the-world

2 http://www.wired.co.uk/news/archive/2011- 05/23/26-terabit-laser

3 http://www.ncoic.org/about-us/interoperability- projects/nga-demonstration

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.

Sung-Yueh Perng is a Postdoctoral Researcher on the Programmable City project, exploring current and emerging collaborations and contestations in the processes of situating codes, software, geodata and mobile devices in their social, spatial and technological configurations. Before joining NIRSA, he worked in Department of Sociology, Lancaster University, on the BRIDGE project, investigating social and ethical opportunities and challenges arising from incorporating social computing into emergency response. He also explored various ways in which routines in everyday life have been (and continue to be) reshaped through the exposure to and engagement with innovative ideas and practices, digital and locative arts, wireless signals and various mobilities systems.

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)._