Privacy, Security, Liberty: Informing the Design of EMIS

Monika Buscher
mobilities.lab, Lancaster University, UK
m.buscher@lancaster.ac.uk

Lisa Wood
Faculty of Health and Medicine
Lancaster University, UK
l.a.wood@lancaster.ac.uk

Sung-Yueh Perng
mobilities.lab, Lancaster University, UK
sy.perng@gmail.com

ABSTRACT

This paper explores issues of security, privacy and liberty arising in relation to ICT supported emergency management. The aim is to inform the design of emergency management information systems (EMIS) and architectures that support emergent interoperability and assembly of emergency management systems of systems. We show how transformations of social and material practices of privacy boundary management create challenges, opportunities and dangers in this context. While opportunities include development of more efficient and agile emergency management models, building on smart city concepts, dangers include surveillance, social sorting and an erosion of civil liberties. Against this backdrop, we briefly explore human practice focused 'privacy by design' as a candidate design avenue.

Keywords

Privacy, security, liberty, emergency management information systems (EMIS)

INTRODUCTION

Three trends in contemporary societies make privacy protection an important issue in the design of Emergency Management Information Systems (EMIS) (Turoff, Chumer, Van De Walle, & Yao, 2003; Van De Walle, Turoff, & Hiltz, 2010; Van De Walle & Turoff, 2007):

- Calls for greater interoperability – inspired by recurring experiences of difficulties of communication, coordination and collaboration in disaster response, and also including calls for support for the assembly of flexible 'systems of systems' for emergency response (US Department of Homeland Security, 2004)
- A digital 'tsunami' – a term coined by an EU Commission 'Future Group', who observe how people and objects can be mapped, tracked and interrogated for commercial, social, and security purposes; how individuals contribute data through self-disclosure, e.g. in social media, and how advances in data processing make this 'tsunami' of personal data amenable to potent analysis (Future Group, 2007).
- Fear of 'big brother' surveillance – fuelled by increasing awareness and unease with privacy intrusion and personal data processing and surveillance.

Together, these three trends create a complex landscape of incentives, opportunities and challenges for EMIS innovation. Faced with life-threatening circumstances, many people would regard a loss of privacy a small price to pay for swift assistance. To speed up search and rescue, or to contain the spread of infectious diseases, personal information such as location and names would clearly be useful (and obtainable even from turned off mobile phones, if telecommunications operators share their data (Bengtsson, Lu, Thorson, Garfield, & Schreeb, 2011). To receive the most appropriate medical care, interoperability with medical records and data from biosensors or implants (such as wireless pacemakers) could be helpful; and to help responders contact family or friends, mobile phone or social media data could be consulted. Personal data can also play an important role in prevention, planning, and recovery phases. For example, surveillance of suspects may help prevent crime, knowledge about persons most vulnerable (e.g. the elderly, chronically ill, or families with young children) may

help emergency response agencies tailor warnings, advice and support to the specific needs of such populations, and access to households' purchasing records could speed up compensation during recovery.

Advanced information and communication technologies (ICT) have the potential to enhance personal data processing capabilities for emergency response, aiding the development of better, more efficient and economical services. EMIS try to leverage this potential. However, how societies, institutions and organizations handle, and how individuals can control, personal data are highly consequential matters, deeply entangling security, privacy and liberty with technological potential. Data protection laws, legal risk analysis, privacy protection practices, policies and technologies are being developed to manage risks and opportunities for individuals, groups, and society as well as professional responders. In this paper we provide an overview of issues to inform the design of EMIS and architectures that support assembly of 'systems of systems' for 'agile' emergency response.

TRANSFORMATIONS OF PRIVACY

Traditional definitions of privacy describe it as a state of social withdrawal or the right to be 'left alone' (Brandeis & Warren, 1890). Over a decade ago, Scott McNealy, then CEO for CISCO, argued that 'You already have zero privacy, get over it' (cited in Langheinrich, 2001), observing that citizens behave in contradictory ways – on the one hand seemingly carelessly sharing personal information, on the other worried about an erosion of privacy. However, privacy is not just a state of withdrawal, but a contextual, situated, practically achieved matter of boundary management (Altman, 1976; Nissenbaum, 2009; Palen & Dourish, 2003). People modulate the disclosure of personal information dependent on the context, controlling it through embodied conduct embedded in material environments, through providing or withholding of information in relations with 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. Palen and Dourish (2003) observe three key boundaries for privacy management:

- Privacy and publicity: 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).
- 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 is important.
- Time/Space: The capability of information technology to transmit and preserve information changes the spatial and temporal 'reach' of information. This creates tension for the control of privacy because how information is going to be used in other places and in the future cannot always be anticipated.

Over the last decade, new areas for privacy boundary management have emerged, most importantly:

- Movement: Smartphones and social network technologies allow friends and family to see where one is, and new uses of database technology complicate selective disclosure of location information (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).
- Social networks: The documentation of social connections in social media can enhance search engines with 'social search' (Sherrets, 2008). This introduces a need for 'social privacy'.

People have developed sophisticated practices of modulating privacy along these boundaries in low-tech, co-present situations, but these practices are based on the ability to understand how one's person is situated and visible in space, time, and in relation to other individuals, groups or organizations. New technologies have engendered a 'steady erosion of clearly situated action' (Grudin 2001, cited in Palen & Dourish, 2003) altering 'our control over how disclosed information is interpreted in different contexts and times', through:

- High-speed transmission – Data can be sent at very high speeds (up to 26 terabits per second[1]).
- Persistence – Data stored digitally can be stored in very large volumes and for very long times.
- Enhanced computation – Abilities of search, triangulation, actuarial analytics, visualizing data and other forms of computation enable sophisticated processing of huge data volumes.

[1] http://www.gizmag.com/record-26-terabits-per-second-data-transmission/18702/

- Disembodiment – The production of and access to personal data are increasingly disembodied. The immateriality of digital information and networks makes it possible for people to generate data without noticing it and for others to access and process such information without their subjects noticing it.
- Dissociation – Dissociation happens when the results of actions are visible, but the actions that led to them are invisible; in other words, when one cannot easily determine who is doing, or did, what. (Bellotti and Sellen, 1993).
- Addressability – A range of generalized and standardized grids and metrics 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). GIS and GPS support this (Crang and Graham, 2007, Graham, 2009, Thrift, 2004), and Internet protocol version 6 (IPv6) makes comprehensive addressability an even more realistic prospect.

For crisis management, ideas of an 'internet of things' (Mattern and Floerkemeier, 2010) helps to locate objects and resources, as well as people who may be trapped or moving away from the scene open up new opportunities for better, more effective and economical disaster management. But the fact that these capabilities are also problematic, because they can obstruct lived practices of privacy boundary management, must be addressed through design, ideally enhancing people's abilities to:

- notice instances of data collection,
- determine who might be looking and why
- comprehend the spatial, temporal, social and political contexts,
- negotiate and agree proportionate and appropriate practices and
- be sure that such agreements are adhered to and, if necessary, enforce them

To support the practices involved in this, privacy sensitive emergency management technology design 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.

CHALLENGES, OPPORTUNITIES, DANGERS

To inform debate about how such support may be developed in and for EMIS, we now review some key challenges, opportunities and dangers that arise from lack of support for privacy management, embedding concerns about privacy in wider consideration of ethical and social issues, focussing on the European Union.

Challenges: Failure to share data, legitimacy and silo-thinking

Experience of the practicalities of data protection in multi-agency emergency response actually highlights 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, for example, points 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 2005, failures to share data amongst the emergency agencies led to inefficiencies and mistakes so significant that the UK Government was prompted to clarify the data protection laws and formulate this specific 'Data Protection and Sharing Guidance for Emergency Planners and Responders'. For example, 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 at a very sensitive time. Such fragmentation of response efforts constitutes an example of 'silo-thinking', or a lack of organizational interoperability, where individual agencies do not collaborate even where this would be useful and possible. The problems are well-known in other countries. Indeed Cole (2010) cites studies where professionals identify 'silo-thinking' as one of the main barriers to organisational interaction.

Opportunities: Systems of systems for agile response

At the same time, transformations of privacy practices allow emergency responders to develop new, more efficient forms of communication, coordination and collaboration. Systems of systems approaches that allow 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)

In the European context, where the emphasis is strongly on 'unity in diversity', the centralization and standardization that drive US efforts are complemented with a subsidiarity principle of devolving decision-making to the lowest possible level (whilst supporting coordinative action at a higher level). This requires support for the situated assembly of appropriate 'adhocracies' and improvisation, 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 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', 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 (Harrald, 2006). The concept builds on visions of 'smart cities' that enable integration of different services, from healthcare to transport management, to insurance, taxation and e-government. There are a number of examples worldwide where such 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 (Maeda, 2010) (Figure 1).

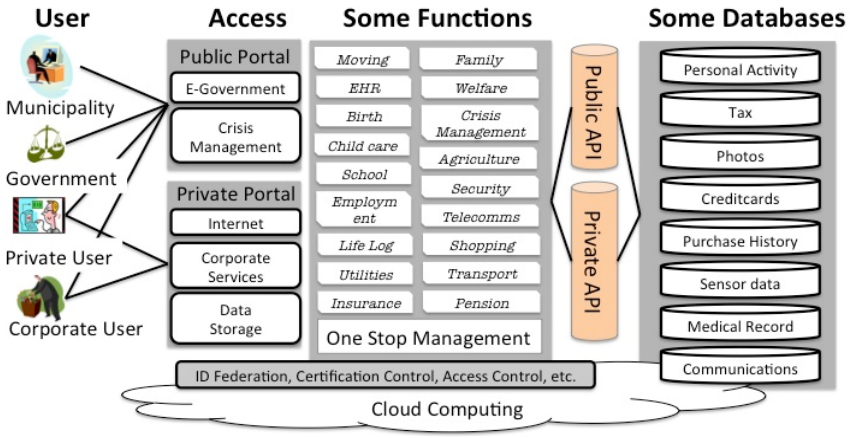

Figure 1 'Next generation ICT services for the resilient society' (adapted from Maeda 2010)

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 define avenues for design, it is important to discuss key dangers in some depth.

Dangers: Surveillance, social sorting, and an erosion of civil liberties

Recent debates about 'Safeguarding Privacy in a connected world' (European Commission, 2012) index 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. Landmark 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 (EU Commission, 2012).

It is critical for designers of EMIS 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 emergency services. Perhaps even more worryingly, technologies may be used in ways that extend surveillance unnecessarily. But to address issues of privacy, security and liberty a deeper understanding of experiences and practices and their implications is needed. The dangers are not easy to circumscribe, they are often hidden and complex. The text in this section seeks to fathom some of the most important, starting with surveillance, exclusionary forms of control, social sorting, false positives, an erosion of freedoms, actuarial justice, retrospective accountability, cultures of fear, and a militarization of emergency response.

With an ever more extensive use of ever more powerful databases, some analysts argue:

… a new Faustian bargain was struck around 1990. … [In a] 'dance with the digital' … [which is] 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 increasing conflicts over resource shortages (water, soil, oil, finance) and climate change, societies face a choice between all-encompassing surveillance and disastrous chaos as global futures 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. The ways in which people and organizations appropriate new technologies, for example, increasingly hybridize public and private aspects of life (Sheller & Urry, 2003). People may, for example, engage in private communications in public spaces, and such communications may be monitored; they have networked medical devices (such as pacemakers) implanted into their bodies, inhabit homes or workspace that are open to scrutiny by others, for example, through assisted living technologies, or media-space technologies. Sherry Turkle states:

we live a life that generates its own electronic shadow. Over time, most people find a way to ignore or deny it. … particularly for those who have grown up in our new regime of surveillance, leaving an electronic trace can come to feel so natural that the shadow seems to disappear. (Turkle, 2011)

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 in relation to EMIS design. Inclusionary discipline occurred, for example, during the 17th Century plague pandemic, a 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, 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, then separation and often permanent exile from society, a form of exclusionary discipline that is one of the points of origin for the exclusionary power of digital profiling techniques that analysts highlight today, where social sorting, categorical exclusion and false positives are critical issues.

Clive Norris' analysis (2002) explains these dangers and their relevance to ICT supported emergency response by mapping Foucault's analysis onto a discussion of how digital surveillance fosters 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. If personal data are stored across such landscapes of interoperable data repositories for commerce, transport, education, administration and crisis response, information about deviance can be searched and stored. It becomes possible to exclude certain groups of people from certain spaces and services. Populations may be diverted and denied access to some services in 'sentient cities', perhaps even without their noticing (Crang & Graham, 2007)(see also Adey, 2009 for an account of preemptive securitization and the body).

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, 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.

Function creep is a danger that can be significantly exacerbated by innovation in EMIS and design for emergent interoperability, because when combined with exceptions to normal data protection rules granted 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, which '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 (locating a trapped victim where there is none, or branding an innocent person as a terrorist suspect, as in the de Menezes case) – can occur. 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). Also, processing might not accurately distinguish noise from important information, leading to false negatives, that is, failing to identify relevant instances (such as a healthy trapped victim or a criminal). These are serious concerns that seriously challenge arguments of 'if you have nothing to hide, you need not worry about surveillance', which are voiced frequently in debates about privacy protection.

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 when may affect the accountability of emergency responders[2] .

Widening our perspective yet further, for societies, the collection and processing of personal data may become problematic because basic rights, such as freedoms of speech, association and movement can be eroded. 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 far-reaching securitization, even 'militarization of everyday life' (Graham, 2010), that is, an embedding of security/military perspectives and technologies into of everyday spaces and everyday lives, from all-surround CCTV to the use of blast proof concrete in buildings. EMIS, too, are embracing military inspired technologies, such as incident command system (ICS) structures and GPS. 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 begin to sell to civilian and public authority users, and create new products that are no longer purely military or purely civilian (Wood, Ball, Lyon, Norris, & Raab, 2006). Pressures of shrinking military budgets no doubt fuel some of this doubling, or re-orientation. But integration of military metaphors and technologies into emergency response is a delicate enterprise. They can deeply and 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 (Birkland, 2009; see also Tierney, 2006).

[2] The verdict contrasts starkly with juridical inertia in relation to a company that was found to have rebuilt antiseismic apartments, using substandard seismic isolators, rendering new buildings vulnerable to future earthquakes. See Jones, T. (2012). Short Cuts. London Review.

A militarization of emergency response and everyday culture also contributes to what Giorgio Agamben describes as a spread of exceptions, often declared to protect national security (Agamben, 2005), where fundamental human rights can be suspended. Agamben's argument is complex and it is beyond the scope of this paper to explore it in detail (readers may find elaboration in (Scheuerman, 2006)). Most importantly, the extension of exceptions is exacerbated by increasing emergent interoperability between existing information systems, EMIS through novel architectures that connect them, e.g. into smart city databases. European history is marked by the devastating experience of two world wars, and the holocaust, which was facilitated by an unprecedentedly effective process of collecting, sharing and processing personal data through an efficient bureaucratic apparatus and culture of surveillance (Arendt, 2004; Bauman, 1989). Totalitarian rule was established in no small part through the evocation of a series of extra-legal 'states of exception', which suspended 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 suspension of fundamental human rights and 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, inform the design of information systems with ever more permeable boundaries between data controllers, persistent storage, and powerful analytic and visualizing capacities, EMIS, smart city systems and 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).

These dangers are, in part, allowed to coalesce, because citizens do not 'feel' the intrusion into their privacy. Pre-emptive measures are often localised, unplanned, enabled by invisible infrastructure and powered by blackboxed interoperability between systems. Genuine and imagined threats and austerity 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 and fearful discourses of security. Our summary of dangers suggests that such advances have the potential to erode democratic citizenship and civil liberties, but it also charts opportunities for intervention through circumspect design and innovative appropriation of EMIS, which we will now consider briefly.

PRIVACY BY DESIGN FOR EMERGENCY MANAGEMENT INFORMATION SYSTEMS OF SYSTEMS

Privacy sensitive agile emergency response is a hopeful vision. Realizing it without breaking fundamental freedoms is a challenging balancing act for design. It is beyond the scope of this paper to resolve the dangers we have explored, but in this section we seek to contribute to larger efforts, by discussing 'privacy by design' 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 & DeHeert, 2012). In our own work, we combine these 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 such (changing) practices.

This approach has shown that inscribing compliance into technologies is less useful in EMIS design, in view of the dynamic nature of emergency management and the need for 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 enforced through rigid regulation, to an understanding of privacy as a contextual value and embodied practice that is augmented and constrained by technologies, cultural conventions and the law. By taking this perspective, alternative 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. Our research suggests that a human practice focused approach is particularly useful for EMIS design in view of the substantive ethical and legal challenges.

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 et al., 2008) 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 et al., 2006)

In the context of emergency response violations of data protection regulations may be necessary and legitimate. Personal data may 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 use of personal data accountable at the time of use and retrospectively seems promising. Weitzner et al (2006) introduce three mechanisms to maintain accountability when performing data mining:

- **Inferencing Engine(s)** that support analysis of data and assesses compliance with relevant rules
- **A Truth Maintenance System** based on a persistent store fed by inference engines checking data accuracy as well as data provenance, and reliability of inferences
- **A Proof Generator** that constructs proofs that critical transitions and unplanned uses of personal information are justified by facts and permissible under applicable rules

This form of privacy protection aims to protect privacy from three directions: (1) by controlling access, (2) by supporting reference to pre-defined rules and (3) by making the justification of inferences trace-able. The transparency and accountability gained is useful for a human practice focused approach, because it can augment practices of utilizing interoperable data stores in times of crisis, whilst supporting awareness of rules and accountability of breaching such rules.

CONCLUSION

The main contribution of this paper is a discussion of key challenges, opportunities and dangers of utilizing personal data for emergency management. We argue that it is important to translate enhanced privacy sensitivity into design and have highlighted privacy by design as a promising avenue for design. In conclusion, 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 professional responders as well as other stakeholders and the public in noticing, negotiating and managing privacy is a more effective and useful approach.

ACKNOWLEDGEMENTS

We would like to thank our anonymous ISCRAM reviewers, and our colleagues in the Centre for Mobilities Research, Lancaster University (http://www.lancs.ac.uk/fass/centres/cemore/index.php) and the Bridge project, especially Lucas Introna, Peter Wahlgren, Matts Ahlsen, Kees Nieuwenhuis, Bernard Van Veelen, and Leonardo Ramirez for discussions of privacy and ethical issues. This research is part of the BRIDGE Project, funded under the EU FP7 Security Theme http://www.bridgeproject.eu/en.

REFERENCES

1. Adey, P. (2009). Facing airport security: affect, biopolitics, and the preemptive securitisation of the mobile body. Environment and Planning D: Society and Space, 27(2), 274-295.
2. Agamben, G. (2005). State of Exception. Chicago: Chicago University Press.
3. Altman, I. (1976). Privacy: a conceptual analysis. Environment And Behavior, 8(1), 7–29.
4. Arendt, H. (2004). The Origins of Totalitarianism. New York: Harvest Books.
5. 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
6. Bannon, L. (2006). Forgetting as a feature, not a bug: the duality of memory and implications for ubiquitous computing. CoDesign, 2(1), 3-15.
7. Bauman, Z. (1989). Modernity and the Holocaust. Contemporary Sociology (Vol. 20, p. 267).
8. Bengtsson, L., Lu, X., Thorson, A., Garfield, R., & Schreeb, J. (2011). Improved response to disasters and outbreaks by tracking ppulation movements with mobile phone network data: a post-earthquake geospatial study in Haiti. PLoS medicine, 8(8).
9. Birkland, T. A. (2009). Disasters, Catastrophes, and Policy Failure in the Homeland Security Era 1. Review of Policy Research, 26(4), 423-438.
10. Brandeis, L. D., & Warren, S. D. (1890). The Right to Privacy. Harvard Law Review, IV, 193-220.
11. 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]
12. Clarke, R. (2009). Privacy impact assessment: Its origins and development. Computer Law Security Review, 25(2), 123-135.
13. 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]
14. Crang, M., & Graham, S. (2007). Sentient cities : ambient intelligence and the politics of urban space. Information Communication Society, 10(6), 789-817.
15. 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.
16. Dodge, M., & Kitchin, R. (2007). Outlines of a world coming into existence: pervasive computing and the ethics of forgetting. Environment and Planning B Planning and Design, 34(3), 431-445.
17. EU 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]
18. European Commission. (2012). Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century. Brussels.
19. Foucault, M. (1977). Discipline and Punish. Allen Lane.
20. Furedi, F. (2006). Culture of Fear. Continuum International Publishing Group Ltd.
21. Future Group. (2007). Public Security, Privacy and Technology in Europe: Moving Forward. http://www.statewatch.org/news/2008/jul/eu-futures-dec-sec-privacy-2007.pdf [Accessed 25 Nov 2012]
22. Graham, S. (2008). Cities Under Siege: The New Military Urbanism. Verso.
23. 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.
24. Kafka, F. (2000). The Trial. Penguin Classics.
25. Langheinrich, M. (2001). Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems, Proceeding UbiComp '01 Proceedings of the 3rd international conference on Ubiquitous Computing

273-291.

26. Maeda, Y., Higashida, M., Iwatsuki, K., Handa, T., Kihara, Y. and Hayashi, H. (2010a). Next Generation ICT Services Underlying the Resilient Society. Journal of Disaster research, 5(6), 627-635.
27. 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), 44-9.
28. 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. Polity.
29. Naphade, M., Banavar, G., Harrison, C., Paraszczak, J., & Morris, R. (2011). Smarter Cities and Their Innovation Challenges. Computer Vol. 44, pp. 32-39.
30. Nissenbaum, H. (2009). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press.
31. Norris, C. (2002). From personal to digital: CCTV, the panopticon, and the technological mediation of suspicion and social control. In D. Lyon (Ed.), Surveillance as Social Sorting. Routledge.
32. 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.
33. 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.
34. Ramirez, L., & Buscher, M. (2012). Domain Analysis - Interoperability and Integration. Bridge project Deliverable D2.2. Available from the authors
35. Scheuerman, W. E. (2006). Survey Article: Emergency Powers and the Rule of Law After 9/11*. Journal of Political Philosophy, 14(1), 61-84.
36. Sheller, M., & Urry, J. (2003). Mobile Transformations of `Public' and `Private' Life. Theory, Culture & Society, 20(3), 107-125.
37. Solove, D. J. (2004). The Digital Person: Technology and Privacy in the Information Age. NY: NYU Press.
38. Solove, D. J. (2008). Data Mining and the Security-Liberty Debate. The University of Chicago Law Review, 75(1), 66-67. SSRN.
39. Thrift, N. (2007). Non-representational theory: space, politics, affect. Routledge.
40. 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.
41. Turkle, S. (2011). Alone Together. Basic Books.
42. Turoff, M., Chumer, M., Van De Walle, B., & Yao, X. (2003). The design of a dynamic emergency response management information system (DERMIS). Journal of Information Technology, 5(4), 1-35.
43. US Department of Homeland Security. (2004). The System of Systems Approach for Interoperable Communications. http://www.safecomprogram.gov/library/Lists/Library/Attachments/144/SOSApproachforInteroperableCommunications_02.pdf
44. Urry, J. (2007). Mobilities. Polity.
45. Van De Walle, B, & Turoff, M. (2007). Emergency Response Information Systems : Emerging Trends and technologies. Communications of the ACM, 50(3), 28-31.
46. Van De Walle, B., Turoff, M., & Hiltz, S. R. (2010). Information Systems for Emergency Management. Armonk, NY: M.E.Sharpe.
47. 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.
48. Weitzner, D. J., Abelson, H., Hanson, C., Hendler, J., Kagal, L., McGuinness, D. L., Sussman, G. J., et al. (2006). Transparent Accountable Data Mining: New Strategies for Privacy Protection. Artificial Intelligence. http://www.w3.org/2006/01/tami-privacy-strategies-aaai.pdf
49. Whittaker, Z. (2011). Summary: USA PATRIOT Act series. ZDNet. http://www.zdnet.com/blog/igeneration/summary-zdnets-usa-patriot-act-series/9233
50. Wright, D. (2010). A framework for the ethical impact assessment of information technology. Ethics and Information Technology, 13(3), 199-226.
51. Wright, D., & DeHeert, P. (2012). Privacy Impact Assessment. Springer Netherlands.