Cloud Ethics for Disaster Response

Monika Büscher
Catherine Easton
Lancaster University, UK
{m.buscher, c.easton}@lancaster.ac.uk

Maike Kuhnert
Christian Wietfeld
Dortmund University of Technology, Germany
{maike.kuhnert, christian.wietfeld}@tu-dortmund.de

Matts Ahlsén
CNet Svenska, Sweden
matts.ahlsen@cnet.se

Jens Pottebaum
Universität Paderborn, Germany
pottebaum@cik.upb.de

Bernard Van Veelen
Thales, Netherlands
Bernard.vanVeelen@D-CIS.NL

ABSTRACT

In emergencies, exceptions to data protection raise concerns that data may become available to unexpected actors during and after a crisis, resulting in privacy intrusion and social sorting. Apart from ethical issues, there are legal issues, for example around data minimization and issues around social and cultural practices of sharing information. This paper explores key ethical, legal and social issues (ELSI) in utilizing cloud computing for disaster response and management and some examples of innovative design.

Keywords

Cloud computing, disaster response and management, ELSI, ethics, common information space, interoperability

INTRODUCTION

> *the lack of a coordinated disaster response caused serious operational and ethical challenges … What unfolded was a massive mismatch and duplication of services (Haiti, Larkin, 2010:495).*

In a world where personal and official post disaster reviews routinely highlight a lack of coordination (ENISA, 2012), the response to the triple disaster in Japan 2011 provides examples that stand out. Amongst the many factors that contributed to successful collaboration there, the disaster 'proved the cloud's ability, efficiency and advantages' (Katsumi cited in Moss, 2013). For example, many local governments' data repositories and IT infrastructures had been damaged. When public authorities needed to provide information, such as radiation measurements, these limited resources received an unmanageable surge of demand. Cloud service providers such as Fujitsu, IBM, and others offered free mirroring, which meant that central and local governments could survive the access storm. Moreover, 'Relief/rescue stuff/goods were enough, but supply-demand matching was impossible without IT: [the] cloud worked!' (Katsumi, 2013). Customer Management Software (SaaS), again offered for free, allowed Non-Governmental Organisations (NGO) to share information on victims and resources. This supported 'agility, scalability, ubiquitous access and remote collaboration' (ibid). This was the first time cloud computing augmented not only business/service continuity for individual providers, but also coordination between different agencies involved in disaster response. Since 2011, this potential has prompted a surge of development in cloud computing for disaster response worldwide. However, this has been accompanied by a surge of privacy and other ethical, legal and social concerns. Experts recognize that utilizing the cloud is also a question of morality, but there is a lack of research that can inform more ethically circumspect innovation. In this paper, we review key challenges and propose some resources for innovative design.

CLOUD COMPUTING FOR DISASTER RESPONSE

Cloud computing is an internet-based paradigm, also referred to as 'utility computing' (Zhou, Zhang, Xie, Qian, & Zhou, 2010), because it turns computing into a flexible resource, available 'on demand'. The concepts refer to a collection of 'services' that are 'virtualized', that is, independent of specific configurations, and redundantly spread across different locations. Users can extend their potentially quite simple hardware and software with Software as a Service (SaaS), Infrastructure, Platform, Data, Network or Security as a ((IaaS, PaaS, Daas, NaaS, or SecaaS) and more. For disaster response, there are a number of benefits:

- *Resilience through redundancy* – data, software and other resources, including whole computing environments can be mirrored in other places and recovered; the only requirements are a broadband internet connection and a sustainable synchronization strategy for local data stores.

- *Connectivity* - Mesh and NaaS services can be used to patch and build network connections.
- *Affordability, flexibility, scalability* – Data processing, storage and other operations in the cloud can reduce the need to invest in costly local solutions, charges only apply to actual time and services used; basic equipment can be augmented with cloud services appropriate to the specific situation, expanding IT surge capacity without the need for huge investment upfront or maintenance during normal times.
- *Common Information Spaces (CIS)* –. Cloud services can support data sharing, storage, transformation, privacy and security for the pooling, aggregation, analysis and visualization of information, which is critical for collaboration in emergency situations and effective risk analysis and preparation.
- *Emergent interoperability* – Cloud services can simplify ad-hoc integration at multiple levels: rescue and volunteer organizations (organizational), information resources (semantic) and IT (technological).
- *Security* – moving to the Cloud can enhance security, because it is more likely that high quality and up-to-date services are being used, and SecaaS can enhance this further.
- *Standardization* – Cloud-based collaboration, data sharing and use of communication standards can contribute to the standardization of emergency response and management practices and more equal levels of safety and security among different states, regions and cities.
- *Efficiency* – Use of the Cloud can facilitate a richer, faster and more broad-based understanding of crisis situations and available resources. Advances in efficiency are supported by the fact that the Cloud can scale up from everyday to disaster use, as this facilitates creative and confident use.

To realize these benefits, advances in related areas are needed. Emergent interoperability between 'adhocracies' of emergency response may involve statutory response organizations, such as the police, fire and ambulance services but also NGOs, environmental experts, affected populations, Virtual Operations Support Teams (VOST), supermarkets, insurances, etc. (Mendonça, Jefferson, & Harrald, 2007). Each party comes with its own information systems, data and devices. To share information, responders need support for flexible assembly and orchestration of a '*system of systems*' appropriate for the specific emergency at hand (NATO, 2006, BRIDGE Project http://www.bridgeproject.eu). The utilization and synthesis of information requires collaboration and information sharing between actors e.g. through *emergency management information systems*, *common information spaces* or *Precision Information Environments* (Boulos et al., 2011; Schmidt & Bannon, 1992; Turoff, Chumer, Van De Walle, & Yao, 2004). And approaches that can safeguard security and privacy, such as *firewalling*, *encryption* and *privacy preserving techniques*, are needed (e.g. Wang, Wang, Ren, & Lou, 2010).

SELECTED ETHICAL, LEGAL AND SOCIAL ISSUES

The technologies underlying these benefits share some qualities that make their use risky for individuals, organizations and societies. They can seem 'immaterial', are highly decentralized, distributed, and complex. Their appropriation engenders unintended (positive and negative) consequences that are ill understood and hard to control. This creates challenges for technology designers, emergency planners, policy makers and users. On the one hand, harmful unintended consequences may be difficult or impossible to fix even once they have been noticed. For example, ascertaining data integrity in cloud computing environments is a formidable task. On the other hand, fear of such intractable challenges obstructs lived creation of technical, but also social and legal solutions to such challenges. Below we explore a selection of particularly significant issues and then consider some opportunities for technological and social, practice-based innovation.

Emergency ethics: Crises necessitate difficult choices, e.g. over who and what to save first. This calls for exceptional powers and permissions. Exceptions to data protection, in particular, raises concerns that data may become available to unexpected actors during and after a crisis. In fact, visions of 'next generation' resilient societies even construct wider sharing as desirable, because knowledge about vulnerable populations might strengthen preventive measures (Maeda et al., 2010). This can undermine privacy and civil liberties, if preventive measures become disciplinary, for example through the withdrawal of insurance for non-compliance. Perhaps even more worryingly, access to a wide range of personal data can enable calculation of who 'deserves' support the most. Such social sorting can be discriminatory, disadvantaging the poor - already the most vulnerable in disasters. At the same time, cloud technologies introduce new ethical opportunities. For example, new forms of capturing and analysing communications allow for more public engagement and deeper learning from post-disaster reviews. A difficulty here is that logs from emergency response efforts are often taken out of context, and analysis is coloured by hindsight and can lead to blame. This, in turn, can diminish professional integrity, introducing fear of liability charges into decision making processes. For example, it may be tempting to delay risky decisions until the next person comes on duty (passing the buck), or even worse, potentially effective but risky choices may disappear from view if individuals feel they will be personally held to account by post-disaster reviews and the public. This discussion highlights that 'we are our tools' (Suchman 2011) and the ethics of cloud supported disaster response is distributed across a confusing array of actors and technologies.

Legal issues. Cloud computing, systems of systems and common information spaces can place personal data in physical and virtual realms where different laws to those in its place of origin apply. It erodes legal concepts such as 'data controller', 'data minimization', 'purpose binding', 'anonymization', because, for example, anonymization cannot be guaranteed to hold when data can be correlated. Zhou et al. (2010) discuss a series of legal acts that enable access and use that is considered unlawful by those who own the data (e.g. US PATRIOT Act and its powers to enforce disclosure of EU citizens' travel data), which creates problems for European providers (Baillie, 2012). Certification of cloud services and content needs to be tackled, and implementation decision makers need to be qualified to judge the legal implications of cloud technologies. The right to universal service may need to be extended to include network connectivity On a different level, IT procurement needs to be adapted to cloud computing; more flexible and (cloud) service oriented procedures need to substitute monolithic large-scale system and hardware oriented bidding procedures. Furthermore, the broader legal context is changing. A new EU General Data Protection Regulation (European Commission, 2012) is being developed against a backdrop of surveillance revelations and a focus on regulating international data transfers. In relation to emergency response, there is a need to embed a framework which recognises both the overarching right to privacy and the need to respond in a timely, effective manner, with international collaboration. Developments need to be based upon a strong notion of proportionality and time sensitive storage of data. In relation to inadvertently discriminatory decisions and digital divides, there is a need to focus upon measures to clarify how existing equality and human rights provisions can be applied to cloud-augmented disaster response and management. Work is being undertaken on this at a broader international level through the United Nations and initiatives such as the Charter of Human Rights and Principles for the Internet (2013). A framework for cloud computing for disaster response needs to draw strongly upon and embed human rights principles in an overt manner, developing alongside and strengthening technology-focused anti-discriminatory legal provisions.

Social issues. Facilitating more and more extensive information flows and access to data stores increases social challenges that already exist. For example, mundane difficulties in working up information sharing agreements as part of emergency planning, and in developing information exchange standards and common semantic models challenge effective utilization of the Cloud. Furthermore, creating environments where information can be pooled, visualized, correlated does NOT make a common information space. Sharing of information alone is 'insufficient to enable the development of a common understanding' (McMaster & Baber, 2012). Dynamic working divisions of labour that enact planned procedures and allow for improvisation mean that people need to be able to negotiate significance and meaning and practically collaborate in relation to information. This requires support for interpretation and sense-making, discretion, partial and temporary disclosure, varied information verification processes, as well as awareness and control over one's audience. It requires support for the exercise of information politics and information superiority – not everybody needs to or should know everything (Schmidt & Bannon, 1992). At the same time, through the use of standards, such as the Unified Incident Command and Decision Support System (UICDS) cloud services provide unprecedented opportunities for integrating information from a wide array of actors, including geospatial information and information from social media and online volunteers (Adam, Shafiq, & Staffin, 2012; Boulos et al., 2011).

SOCIO-TECHNICAL OPPORTUNITIES FOR INNOVATIVE DESIGN

The experiences in Japan in 2011 have inspired innovative design that seeks to address these issues and realize the benefits of cloud computing responsibly. In 2013, the US Network Centric Operations Industry Consortium (NCOIC) organized a real-time cloud computing demonstration for the National Geospatial-Intelligence Agency. A re-play of the response 2010 Haiti earthquake showed how organizations from different parts of the world, 'all using different technologies and applications - can supply and retrieve critical geospatial information to meet a range of needs' with cloud computing support (NCOIC, 2013). European innovation efforts in ethically, legally and socially circumspect cloud computing solutions are underway in individual commercial organizations (Jenkins, 2013) and industry-research collaborations, e.g. BRIDGE, and SecInCore. An important aspect of these approaches is to develop social, organizational, and technical innovation together, and we discuss a selection of particularly promising examples.

First things first: Networks in crises. During crises, communications infrastructures are often destroyed or severely congested. Therefore, a key challenge is to set up or rebuild connectivity. Secure wireless mesh networking can provide reliable high performance and low cost ad hoc disaster networks. This technology already has attention from various rescue organizations (Wolff, Sbeiti, & Wietfeld, July 2012), but the main problem, how to place mesh nodes efficiently in crisis situations is not integrated in current processes or standardized yet. Wolff et. al propose to integrate wireless relays in fire hose couplings, so the first responder needs no special training to set up the network and the relays cover the whole incident scene. In addition, the Position Aware Secure And Efficient Mesh Routing Protocol (PASER) (Sbeiti, Pojda, & Wietfeld, Sep. 2012) has been proposed to secure the routing process in the mesh network and to guarantee reliability of data

transmission from sender to destination. Besides secure mesh networks, enhanced mobility support and reliability can be achieved by providing seamless data roaming between communication networks. Further, Movable and Deployable Resource Units (MDRU) (Sakano, et al., 2013) are a step towards disaster resilient networking 'universal service', typically providing various wired and wireless networks within two days of placement. To speed up rebuilding, the patching and use of existing ICT devices and networks to deploy new on the scene ad hoc networks is also a possibility (Al-Akkad et al., 2013). Ideally systems should be able to scale from a dynamically deployed Mesh network with cloud connectivity down to local WiFi or 3/4G networking (and even to using "runners" with off-line storage for upload at the closest command and control post).

Organizational Approaches to ELSI Sensitive Innovation. Informed by visions rooted in European values and pressed by their states and customers, companies are developing solutions that address ELSI in disaster response and management. CloudSigma, a Swiss operator, guarantees customers 'sole root/administrative access over their computing' and integrates advanced technical security solutions such as forward secrecy ECDHE for SSL on HTTPS connections. This means that customers 'are not vulnerable to retrospective decryption using one master private key' (Jenkins, 2013), protecting data from unexpected use. The company also ensures that 'each cloud location is managed by a local company and therefore subject only to [its respective country's] jurisdiction' (ibid.). Mechanisms such as oblivious transfer and privacy-preserving public auditing can complement security and dependability in federated cloud environments, so that international collaboration can accommodate different values, regulatory interpretations and legal conditions whilst realizing the potential of cloud coordination (Kapitza, Schunter, Shapiro, Verissimo, & Waidner, 2012; Zhou et al., 2010).

Standardization: Security Assertion Markup Language (SAML) for Cloud Security. The development of global or industry standards, such as the Emergency Data Exchange Language (EDXL) can be extended with security standards, such as SAML - a proven approach for modeling security and enhancing the binding between identities and authorization information. This binding is suitable for role based security concepts and single sign on (SSO) solutions, used for interaction with decentralized CIS-Services. For example, SAML is used in the project Sec2 (www.Sec2.org) that enables user based encryption/decryption of data and secure communication with cloud based services, also when using an insecure channel for data transmission.

Social, Practice-based and Technical Support for Human Management of Data security and Privacy. Constructing CIS for disaster response comes with the need to develop role concepts that translate between different formal structures in different emergency and volunteer organizations and that provide mechanisms for role improvisation. This role management is needed to provide data security and privacy to involved persons and useful information to rescue personnel. On the one hand, role concepts have to consider the structures of each organization and on the other hand, links between organizations as well as boundaries and independence from each other has to be addressed with role concepts for interoperability. The linking between organizations and their roles in the CIS should be agreed upon in pre-disaster phases. During a crisis the integration of volunteers and non registered personnel has to be supported. This need for ad-hoc adjustment highlights that more data- and infrastructure-centred support is also needed, such as visualization of system of system data flows and annotated workflows (Wood, Büscher, van Veelen, & van Splunter, 2013). Human information practices require that people can see where information is held and who can see what. CIS should support construction and understanding of complex, dynamic informational landscapes, not uniform 'oceans' of data.

CONCLUSION

Cloud computing is an integral part of viable business models in many sectors today. From a technical and operative perspective the benefits of a cloud-supported crisis response and management process lie in the rapid deployment of information services and resource management capabilities. However, the "first mile" still remains critical, i.e., the first responders' interface with the cloud depends on reliable networks. Moreover, from an organizational and multi-agency perspective the benefits are less clear. The lack of commonly agreed upon domain concepts, roles, models and information agreements continue to be an obstacle to semantic and organizational interoperability. Cloud computing can help to overcome technical and syntactic interoperability problems and be a driver for standardization to support cooperation between the different actors (government, commercial, citizen) that need to collaborate in a crisis, but organizational and semantic interoperability issues pose serious challenges. Ethical, legal and wider societal issues further cloud the picture for cloud computing – on the one hand facilitating complex transformations of the service through more agile engagement with affected populations and online volunteers, on the other engendering undesirable unintended consequences such as an erosion of privacy and new digital divides. Innovation efforts that seek to address ethical, legal, social and societal issues as part of developing cloud computing for disaster response provide some examples of how the actors involved can respond to these challenges and opportunities. But a viable framework for cloud computing for disaster response needs to draw more strongly upon analysis of ELSI and develop technical solutions that are more closely integrated with legal, policy, organizational and social innovation.

ACKNOWLEDGMENTS

This research is part of the BRIDGE Project, http://www.bridgeproject.eu/en and the SecInCoRe Project, both funded under the European FP7 Security Theme.

REFERENCES

1. Adam, N. R., Shafiq, B., & Staffin, R. (2012). Spatial Computing and Social Media in the Context of Disaster Management. *IEEE Intelligent Systems*, 27(6), 90–96.
2. Al-Akkad, A., Ramirez, L., Denef, S., Boden, A., Wood, L., Büscher, M., & Zimmermann, A. (2013). "Reconstructing normality." In *Proceedings of OzCHI'13* (pp. 457–466). New York, USA: ACM Press.
3. Baillie, P. (2012). Can European Firms Legally Use U.S. Clouds To Store Data? Forbes 1st February 2012.
4. Boulos, M. N. K., Resch, B., Crowley, D. N., Breslin, J. G., Sohn, G., Burtner, R., Chuang, K. S. (2011). Crowdsourcing, citizen sensing and sensor web technologies for public and environmental health surveillance and crisis management. *International Journal of Health Geographics*, 10(1), 67-96.
5. Charter of Human Rights and Principles for the Internet (2013) http://internetrightsandprinciples.org/wpcharter/ [Accessed 20/01/14]
6. ENISA. (2012). Emergency Communications Stocktaking. http://www.enisa.europa.eu/media/news-items/report-looks-at-improving-emergency-communications [Accessed 20/01/14]
7. European Commission COM (2012) 11. Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data (General Data Protection Regulation).
8. Jenkins, R. (2013). Your privacy is really important to us; this is how we protect you, the customer. JUNE 26, 2013 Cloudsigma. http://www.cloudsigma.com/2013/06/26/your-privacy-is-really-important-to-us-this-is-how-we-protect-you-the-customer/ [Accessed 20/01/14]
9. Kapitza, R., Schunter, M., Shapiro, M., Verissimo, P., & Waidner, M. (2012). Security and Dependability for Federated Cloud Platforms. *Dagstuhl Reports*, Vol. 2, Issue 7. (pp. 56–72). Dagstuhl.
10. Katsumi, B. T. (2013). The Resiliency, Dependability and "Survivability" of Cloud Computing. http://www.cloudscapeseries.eu/Content/Agenda.aspx?id=264&Page=1&Cat=0!2!1 [Accessed 20/01/14]
11. Larkin, G. (2010). Unwitting partners in death - The ethics of teamwork in disaster management. *The Virtual Mentor: VM*, 12(6), 495–501.
12. Maeda, Y., Higashida, M., Iwatsuki, K., Handa, T., Kihara, Y., & Hayashi, H. (2010). Next Generation ICT Services Underlying the Resilient Society. *Journal of Disaster Research*, 5(6), 627–635.
13. McMaster, R., & Baber, C. (2012). Multi-agency Operations. *Applied Ergonomics*, 43(1), 38–47.
14. 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.
15. Moss, J. (2013). Cloud Shines Brightly as Future of Disaster Response IT - NJVC. NVJC. http://www.njvc.com/solutions/cloudcuity/cloud-computing-disaster-response [Accessed 20/01/14]
16. NATO. (2006). Interoperability for joint operations. Retrieved from http://www.nato.int/docu/interoperability/interoperability.pdf [Accessed 20/01/14]
17. Sakano, T., Fadlullah, Z.M., Ngo, T., Nishiyama, H., Nakazawa, M., Adachi, F., Kato, N., Takahara, A., Kumagai, T., Kasahara H. and Kurihara, S. (2013) Disaster-Resilient Networking: A new vision based on movable and deployable resource units. *IEEE Network*, pp. 40-46, July/August 2013.
18. Sbeiti, M., Pojda, J. and Wietfeld, C. (2012) Performance Evaluation of PASER - an Efficient Secure Route Discovery Approach for Wireless Mesh Networks. *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications - PIMRC*, Sydney, Australia, Sep. 2012.
19. Schmidt, K., & Bannon, L. (1992). Taking CSCW seriously. *CSCW*, 1(1), 7–40.
20. Suchman, L. (2011) Consuming anthropology. In *Interdisciplinarity: Reconfigurations of the Social and Natural Sciences*. Eds A. Barry & G. Born, Routledge, London.
21. Turoff, M., Chumer, M., Van De Walle, B., & Yao, X. (2004). The design of a dynamic emergency response management information system (DERMIS). *Journal of Information Technology Theory and Application*, 5(4), 1–36.
22. Wolff, A., Sbeiti, M. and Wietfeld, C. (2012) Performance Evaluation of Process-Oriented Wireless Relay Deployment in Emergency Scenarios. *IEEE Symposium on Computers and Communications - ISCC*, Cappadocia, Turkey, July 2012.
23. Wood, L., Büscher, M., van Veelen, B., & van Splunter, S. (2013). Agile Response and Collaborative Agile Workflows. International Journal of Information Systems for Crisis Response and Management, 5(3), 1–19.
24. Zhou, M., Zhang, R., Xie, W., Qian, W., & Zhou, A. (2010). Security and Privacy in Cloud Computing: A Survey. In 2010 *Sixth International Conference on Semantics, Knowledge and Grids* (pp. 105–112). IEEE.