# Chapter 13
# Privacy, Security, and Liberty:
## ICT in Crises

**Monika Büscher**
*Lancaster University, UK*

**Sung-Yueh Perng**
*National University of Ireland, Ireland*

**Michael Liegl**
*Lancaster University, 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 socio-technical 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.*

## 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 trade-off 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.

# Related Content

Ethical Considerations in the Educational Use of Generative AI Technologies
Burak Tomakand Aye Ylmaz Virlan (2024). *Exploring the Ethical Implications of Generative AI (pp. 49-62).*
www.irma-international.org/chapter/ethical-considerations-in-the-educational-use-of-generative-ai-technologies/343698

Intentionally Secure: Teaching Students to Become Responsible and Ethical Users
Judith L. Lewandowski (2019). *Emerging Trends in Cyber Ethics and Education (pp. 118-130).*
www.irma-international.org/chapter/intentionally-secure/207664

Is It Privacy or Is It Access Control?
Sylvia L. Osborn (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications  (pp. 1133-1141).*
www.irma-international.org/chapter/is-it-privacy-or-is-it-access-control/228772

Government's Dynamic Approach to Addressing Challenges of Cybersecurity in South Africa
Thokozani Ian Nzimakwe (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications  (pp. 139-156).*
www.irma-international.org/chapter/governments-dynamic-approach-to-addressing-challenges-of-cybersecurity-in-south-africa/228725

Role of Cyber Security and Cyber Forensics in India
Gulshan Shrivastava, Kavita Sharma, Manju Khariand Syeda Erfana Zohora (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications  (pp. 1349-1368).*
www.irma-international.org/chapter/role-of-cyber-security-and-cyber-forensics-in-india/228787