European states increasingly rely on digital personal data to manage security — and safety risks. Information and communication technology facilitates the collection and processing of digital personal data for risk profiling purposes. Based on the outcome of the analysis, people are categorized according to their predefined levels of potential threat. Thus financial and traveler’s data or online behavior are becoming a valuable asset of risk management. Human rights, such as the right to privacy, are widely assumed to be affected by these changes. These developments inspired the University of Amsterdam to organize the Amsterdam Privacy Conference in 2012. During this interdisciplinary academic gathering several ‘privacy and security’ panels were organized. The articles in this special issue ‘Security versus Privacy: What is Europe heading for?’, were discussed in these panels. Some were part of a debate on increased surveillance and information security in Europe, whereas others focused on data protection, identification and strategy.

International organizations including the Organization for the Security and Co-Operation in Europe (OSCE) have for decades raised awareness and set standards on security and privacy. The OSCE regularly emphasizes the need for privacy and data protection in the context of, for example, a comprehensive approach to cyber security or the freedom of the internet. Whereas the European Union (EU), is currently drastically revising its data protection legislation to protect online privacy in order to set international renowned standards for the processing and movement of personal data.

For the OSCE the issue of privacy and security remains crucial, because it is one of the most thought-provoking dilemmas of our digital time. Data mining, for instance, enables public and private authorities to provide for safety and security in a more sophisticated manner. This, however, provokes questions about human rights compliance. What are, for example, the (side) effects of monitoring social media for the right to privacy? A key question in the European context is: What are the new risks and challenges for privacy and data protection emerging from changing security technologies and practices? Moreover, how are these risks checked and balanced by accountability mechanisms? Should there be a difference between accountability for public and private authorities?

In this special issue these questions are addressed by focusing on accountability, safety and security concerns in relation to the practices of open source information collection and the introduction of smart surveillance systems.

---

1 Guest editor of this special issue of Security and Human Rights, Quirine Eijkman (PhD) is a senior researcher / lecturer at the Centre for Terrorism and Counterterrorism (CTC), Leiden University-Campus the Hague.
as well as by reflecting on transatlantic data exchange and the new draft data protection legislation proposed by the European Commission in January 2012.

Several concepts including privacy and data protection are referred to by the authors. What do they entail in the context of ‘new’ safety and security threats in Europe? For example, are mass surveillance measures such as Closed-Circuit Television (‘CCTV’) cameras, technology for DNA or fingerprint recognition and data storage or data mining programs including Passenger Name Records (‘PNR’) justified to anticipate and prevent common threats? Which safety and security concern does Europe have to deal with? According to the EU Internal Security Strategy\(^2\) they constitute among others terrorism, serious and organized crime, cyber-crime, etc.

In our digital era privacy and data protection are key human rights. Basically, privacy fundamentally implies the respect of public and private authorities for the personal life of individuals’ domestically or in — digital — correspondence to each other. According to article 8 of the European Convention of Human Rights, interference with privacy within a democratic society is allowed, but only on the basis of a law and when particular criteria, such as the interest of national security or public safety, apply. Yet privacy is more than just law, it is a key value of society and influenced by culture. Ethical hackers, for instance, probably have a different sense of information security than law enforcement officials do. Personal data is related to the collection of personal information about individuals (the ‘data subject’), gathered under particular conditions and for legitimate purposes. Data protection law obligates public or private actors to protect all data that can identify a person. Thereby it obliges them to actively safeguard personal data after it has been collected, processed, stored or transferred.

During the last decade, due to innovative information and communication technology, the context of privacy protection has changed drastically.\(^3\) The threshold to collect, access, process and transfer — digital — personal data for security and safety purposes has lowered and legislation needs to be updated. From a safety and security perspective innovative monitoring and surveillance technologies are to be welcomed. Nonetheless, the (side) effects for the democratic society and the protection of citizen’s rights have to be taken into account as well. Questions that need to be addressed include: How transparent is the design and use of security technology in Europe? For example, is the access to one’s personal data or information about its international transfer granted? Are accountability mechanisms for public and private authorities future-proof? All the contributors to this special issue address one or more of these security and privacy concerns, thereby contributing to the debate ‘what is Europe heading for?’
