SECURITY AND HUMAN RIGHTS
MONITOR

Security versus privacy

What is Europe heading for?

Quirine Eijkman
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.

DOI: 10.1163/18750230-99900032

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 isone 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 Europeancontext is: What are the new risks and challenges for privacy and data protection emerging from changing security technologies and practices? Moreover, how arethese risks checked and balanced by accountability mechanisms? Should there bea 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 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 NameRecords ('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[1] 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 Conventionof Human Rights, interference

[1] Council of the European Union, *Internal Security Strategy for the European Union: Towards an European security model,* 2010, no. 5842/2/2010.

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 particularconditions 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.[2] 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 isthe 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? Areaccountability 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?

Quirine Eijkman and Daan Weggemans discuss the accountability for opensource information collection by intelligence and security agencies and the police. Increasingly, public authorities are using messages on social media websites, weblogs, chat rooms or smart phone apps to gather intelligence. This occurs while state accountability mechanisms have found it difficult to adapt to the online open source culture. From a human rights perspective, open source intelligence collection by public authorities requires proper checks and balances.They conclude that state accountability should focus not only on new legislation,but also on the actual process and outcome of data collection, processing, miningand sharing.

Privacy and data protection in relation to European 'smart' security technologies and policies is considered by Mathias Vermeulen and Rocco Bellanova. 'Smart' surveillance is popular among computer scientists and European policy makers. While there is currently no accepted legal definition of 'smart' surveillance, the term generally refers to the use of computer vision and/or pattern recognition technology to analyse 'big data' to enable semi-automated decisions. The contribution suggests, on the basis of two case studies,namely the EU PNR project and the EU's 'smart borders' initiative, that smart surveillance technology leads to new human rights concerns. The reason for this is that the promise of sifting out relevant information, data minimalisation and the neutral targeting of a surveillance subject is, in reality, more complex than often assumed.

Andreas Busch analyses the transatlantic data exchange from a political science perspective. In spite of the ideas of the original creators of cyberspace, who had hoped for freedom from state regulation, states have continued to play an important regulatory role. Nonetheless, privacy legislation with respect to cross-border data flows is fraught with the difficulties of collective action problems and different national security and safety priorities. The article considers negotiations between the United States and the EU in relation to the 'safe harbor' agreement, the dispute about the PNR transfer and access to financial data (SWIFT). It concludes that

[2] H. Nissenbaum. *Privacy in Context: Technology, policy and the integrity of social life,* 2010, Stanford.

the context of cross-border data flows has changed and subsequently the dominant constructivist approach of the political sciences should be complemented by an analysis of the interests of the negotiation partners as well as the institutional factors that are at play.

Finally, Gloria González Fuster's contribution discusses the significance ofthe draft EU personal data legislation. By examining its impact on the articulationof EU personal data protection law and security, which was until now profoundlyindebted to the link between personal data protection law and the right to privacy, the article reviews the main uncertainties of the current status of the EU fundamental right to personal data protection. Furthermore, it explores the implications of placing EU personal data protection under the (still) unstable right of personal data mining and profiling by law enforcement and security and intelligence agencies.

This special issue contributes to the debate about the future of the right to privacy in the context of 'new' safety and security concerns in Europe. Surveillance technology and information exchange are key tools in the fight against terrorism, serious and organized crime, cyber-crime, etc. They are used by public and private authorities to anticipate risks and perhaps even prevent crime or serious public disorder. However, human rights concerns arise because of the lower threshold to collect, store, mine and exchange digital personal data. Accountability mechanisms increasingly address this by focusing on data protection criteria including data minimalisation, purpose limitation, proportionality, subsidiarity, data subject rights, adequate protection and compliance by private companies. However, in the context of safety and securitythis is challenging, especially because public authorities prefer to be exempted from these obligations. Henceforth, European states need to determine the level of accountability that is required to comply with their privacy responsibilities in the context of security.

This article was first published with Brill | Nijhoff publishers, and was featured on the Security and Human Rights Monitor (SHRM) website.

Security and Human Rights (formerly Helsinki Monitor) is a journal devoted to issues inspired by the work and principles of the Organization for Security and Cooperation in Europe (OSCE). It looks at the challenge of building security through cooperation across the northern hemisphere, from Vancouver to Vladivostok, as well as how this experience can be applied to other parts of the world. It aims to stimulate thinking on the question of protecting and promoting human rights in a world faced with serious threats to security.

Netherlands Helsinki Committee
Het Nutshuis
Riviervismarkt 4
2513 AM The Hague
The Netherlands

© Netherlands Helsinki Committee. All rights reserved.

www.nhc.nl