Journal of Politics and Law; Vol. 6, No. 4; 2013
ISSN 1913-9047 E-ISSN 1913-9055
Published by Canadian Center of Science and Education

Digital Security Governance and Accountability in Europe: Ethical Dilemmas in Terrorism Risk Management

Quirine Eijkman[1]

[1] Centre for Terrorism and Counterterrorism (CTC) Leiden University-Campus The Hague, the Netherlands

Correspondence: Quirine Eijkman, Centre for Terrorism and Counterterrorism (CTC) Leiden University - Campus The Hague, the Netherlands. E-mail: q.a.m.eijkman@cdh.leidenuniv.nl

Received: November 4, 2013 Accepted: November 18, 2013 Online Published: November 29, 2013

doi:10.5539/jpl.v6n4p35 URL: http://dx.doi.org/10.5539/jpl.v6n4p35

Abstract

Digital security governance – the use of digital personal data for threat analysis on the basis of (automated) risk profiling – enhances terrorism risk management in Europe. European security strategies emphasise that information and communication technology increasingly play a key role in preventing and anticipating threats such as terrorism and cyber-crime. It enables, for example, the sharing of personal, financial or travellers' data with third countries. This article focuses on digital security governance in the context of the Passenger Name Record (PNR), the Advance Passenger Information (API) and the Terrorist Finance Tracking System (TFTP) programmes. Particularly, it considers the ethical dilemmas of using and sharing digital personal data as well as accountability for this type of risk management. Because there are broader socio-political, legal and technological issues connected to the use of information and communication technology for digital security governance, the concept of accountability in this article is holistic.

Keywords: digital security governance, European Union, terrorism risk management, accountability, data protection, risk profiling, Passenger Name Record (PNR), Terrorist Finance Tracking System (TFTP)

1. Introduction

European states strongly rely on innovative technological tools to manage the risk of terrorism. New information and communication technology, facilitates digital security governance, which entails the collection, processing, storage and sharing of digital personal data for risk profiling (Valverde & Mopas, 2004; Valverde, 2003). (Note 1) On the basis of this data, people are categorised according to a (pre-defined) level of potential threat. Across the world, no-fly lists, crime or serious nuisance prediction systems, biometric immigration databases as well as youth intervention databases emerge. Personal information about data subjects is collected, mined, stored, and transferred by public and private authorities. Hence, digital personal information such as financial or traveller data has become a valuable asset for risk management in the field of counter-terrorism. The European Internal Security Strategy emphasises that information and communication technology is an important tool in preventing or anticipating threats such as terrorism, cyber-crime, and serious or organised crime. One of the reasons for this is that those who pose a security risk (e.g., criminals, terrorists) are believed to adapt quickly to changes in technology. The strategy furthermore stresses that security governance is based on shared common values including the rule of law and Human Rights Council of the European Union (CEU) (2010a/b/2008/ 2007a/ 2005/2003). States assume that terrorism can be more effectively prevented and countered with innovative information and communication technology. One of the underlying reasons is the fact that digital personal information has become more widely available and shared. Cyberspace, which includes computers, mobile and landline networks linking people throughout the world to communicate and exchange information, facilitates the collection of digital data for security governance (Note 2) in an unprecedented manner. Additionally, the costs involved in using these technological tools are relatively low. Hence, digital personal information is considered to be a valuable and economical asset of terrorism risk management. It has led to the creation of large-scale European Union (EU) databases and improved information-sharing between Member States and third countries. In fact, several recent security-related measures such as the Passenger Name Record (PNR), the Advance Passenger Information (API) and the Terrorist Finance Tracking System (TFTP) programmes indicate that digital personal data have become an important part of EU security policies.

Simultaneously, new questions arise about ethical dilemmas in relation to security governance and especially

regarding digital personal data and information-sharing. Consider, for example, how algorithms of risk profiles for travellers are constructed: What if someone is erroneously labelled as a high risk individual on the basis of incorrect personal information that is automatically generated, and is not allowed crossing a border based on such information? Even if this person knew the cause of the misinformation, does he or she have the right to correct the information that led to this travel restriction? And, which entity or person is accountable for this mistake? This illustrates that the use and sharing of digital personal data for terrorism risk management comes hand in hand with side effects. Even though public and private accountability for digital data protection is currently a hot topic within the EU, (Note 3) there are still unresolved accountability concerns. (Note 4) By focusing on the case studies of PNR and TFTP, this article explores digital security governance in a European context. Especially the ethical dilemmas of using and sharing digital personal data as well as the possibility for accountability for this form of terror risk management are discussed.

2. Digital Security Governance and Terrorism Risk Management

The concept of security governance may mean different things to different audiences: Politicians, policymakers, law enforcement officials, and security officials each have their unique understanding of what should be governed (national borders, cyberspace, vital infrastructure), who is being governed (EU citizens, migrants) and who is responsible (public or private actors) (Ceccorulli, Fioramonti, Hanau Santini & Lucarelli, 2010). Following Kirchner (2007, 3), security governance in this article is understood as an 'intentional system of rule that involves the coordination, management and regulation of issues by multiple and separate authorities, interventions by both public and private actors, formal and informal arrangements and purposefully directed towards particular policy outcome'. For over a decade, security governance has been influenced strongly by a desire to anticipate the threat of terrorism. The precautionary principle, which not only entails the prevention of adverse effects, but also a situation of anticipating potential risks, has become influential in the governing of European security (Hilty *et al*., 2005; Von Schomberg, 2006; Wright, Gellert, Gutwirth & Friedewald, 2011). Various actors such as governments and private security companies use (or facilitate the use of) the sharing of digital personal data as a tool to coordinate, manage or regulate a particular issue (the risk of terrorism) and expect a policy outcome (reducing the threat).

This article particularly discusses one aspect of security governance: the governing of security and safety risks by information-sharing and information-processing on the basis of digital personal data. As Gruszczak (2010) argues, in the post-9/11 era, information and communication technology has dramatically changed how security is governed. The threshold to, for example, share intelligence or (digital) personal data between public and private actors has been lowered significantly. American President Obama, for instance, recently signed an executive order, the Cyber Intelligence Sharing and Protection Act, that enables cyber security information-sharing between the government and private companies who are vulnerable to hacking and/or in charge of vital infrastructure. In this article the use of digital personal data for threat analysis on the basis of (automatic) risk profiling is understood as 'digital security governance'. Conceptually, digital security governance is closely linked to 'targeted governance', which is a way of governing security and safety through risk factors that identify and evaluate high-risk indicators of people's physical locations or cyberspace activities (Valverde & Mopas, 2004; Valverde, 2003). Thus, governance is exercised by relying on digital information of people (so-called data subjects), which is collected, stored, mined and/or transferred. The outcome facilitates the identification of risk factors and threat analysis.

Digital security governance enhances terrorism risk management. Within the EU, personal information including travel or financial data is shared with third countries such as the United States (US). Even though intelligence and security agencies as well as law enforcement offices have always collected and exchanged personal information of individuals that potentially pose a threat, political support and developments in information and communication technologies have led to revolutionary data retention measures as well as unprecedented information-sharing efforts since 9/11 (Archick, 2012; De Goede, 2008; De Vries, 2005). More and more personal information is stored and shared with third countries by a variety of public and/or private agencies. The EU, for instance, was requested by the US to interconnect its internal security network with the US Department of Homeland Security (Pawlak, 2007). Thus, the pool of potentially valuable digital personal data to counter terrorism has increased.

Moreover, databases no longer store personal information on the selected few, but focus on a larger pool of potential suspects. In Europe there are large-scale databases for security and safety purposes; and information-sharing among national and third authorities has become easier. (Note 5) Data mining methods such as big data analysis have become more sophisticated, which has in turn facilitated smart profiling 'capable of extracting application-specific information from captured information (be it digital images, call logs or electronic

travel records) in order to generate high-level event descriptions that can ultimately be used to make automated or semi-automated decisions' (Vermeulen & Bellanova, 2012; Wright *et al*., 2010). This may include smart surveillance camera systems, which are programmed to detect 'abnormal' behaviour at train stations or airports, or programmes for online surveillance of violent extremism that could flag down jihadist propaganda websites. Henceforth, as automated decision making is becoming an accepted practice for terrorism risk management, detailed personal data of all European citizens is shared with third countries, initially often on an ad hoc basis, in order to detect potential terrorists (Balzacq, 2008; Müller-Wille, 2008).

3. Terrorism Risk Management in Practice

During the last decade, digital security governance has grown in importance and has led to the creation of a number of terrorism risk management programmes, which are based on the storage, processing and transfer of digital personal data. According to the EU Internal Security Strategy, digital personal data are increasingly an asset in the fight against terrorism (CEU, 2010a). Initially European states and companies responded by collecting and transferring digital personal data to the US, mainly because the majority of these counter-terrorism programmes were created by the US government. However, for the past few years, the EU has been developing its own digital security governance initiatives. In this section, several case studies, namely the PNR, the API and the TFTP, are introduced. This in order to facilitate the discussion of the ethical dilemmas of collecting, processing and transferring digital personal data for terrorism risk management purposes in Europe.

3.1 Digital Traveller Data: Storage, Processing and Transfer

The storage and transfer of EU airline passengers' data is currently a hot topic in the digital security governance debate. In this case study, both the transfer and the processing of digital personal data to the US Department of Homeland Security, which is based on a re-negotiated international agreement from 2012 ('EU/US PNR agreement' (Note 6)), and the proposal for the EU's own PNR system are introduced (EC, 2011a; CEU, 2011). In 2011 the European Commission resubmitted a 2007 proposal for an EU PNR Directive,which indicates that Member States must transfer PNR data of international flights to and from Member States as well as the processing of that data, which includes its collection, use and retention by the Member States and its sharing between them.

For a number of years, a limited number of states were using PNR data to address serious crime and terrorism, but due to the on-going development of information and communication technology, this data has been used more extensively and systematically. PNR is the (digital) passenger data that airlines collect from their passengers when they make a flight reservation. The data, which is mainly stored in databases of Computerised Reservation Systems, contain records of flight numbers, travel dates, ticket information, limited contact details, travel agents (if applicable) and type of payment (Brouwer, 2009; Hasbrouck, 2009). Airlines are only obliged to disclose information they have collected, there is no obligation to ask for additional information. Initially, PNR was intensified after a series of air flight hijacks in the 1960s. Following 1968, 'various anti-terrorist and anti-crime security measures in civil aviation were adopted worldwide, and air passenger data became one of the most important sources for surveillance in the context of air traffic' (Mironenko, 2010). At first, for security purposes, the luggage controls intensified. Later on, the first Computer Assisted Passenger Pre-screening System (CAPPS) was implemented in the US in the late 1990s, which allowed for the automatic designation of possibly suspicious individuals and a stricter screening of those. Nowadays PNR data is analysed 'in conjunction with current intelligence to identify high-risk travellers before they board their flights' (House of Lords, 2007, 7).

After 9/11, intensified security measures were taken in the aviation sector, leading to the implementation of the PNR requirement in the US. As a result, all international airlines had to transfer detailed passenger data, which is registered on the airline's computer systems, of all passengers to the US Bureau of Customs and Border Protection. In March 2003, the US government announced that non-compliance, meaning the non-provision of such PNR data to the US authorities, would lead to a fine for the air carrier and the revocation of US-landing authorisation (Archick, 2012). As the (forced) disclosure of PNR data of citizens of the EU by airlines was considered a breach of EU legislation, bilateral agreements were created between EU Member States and the US Department of Homeland Security to 'push' a maximum of 34 of already collected data elements of travellers to the US-PNR system (Byrne, 2012; CEU, 1995). These include, among others, passenger names, addresses, telephone numbers, seat numbers as well as more sensitive data such as religious meals or medical conditions. From 2004 onwards, the EU and the US negotiated a time-limited agreement for the provision of PNR data. This agreement, however, was contested and annulled in 2006 by the European Court of Justice (ECJ) because of a lack of appropriate legal basis (European Court of Justice (ECJ), 2006). A new bilateral agreement was approved by the Council of the European Union (EU Council) in 2007. This was provisionally in force and entailed a push

of maximum 19 instead of 34 already collected data elements. In 2010 the European Parliament appealed successfully to the European Commission to renegotiate the 2007 US-EU PNR agreement (European Parliament (EP), 2010). Subsequently in 2012, it approved a renegotiated bilateral agreement on the transfer of PNR data via the US Bureau of Customs and Border Protection to the US Department of Homeland Security; this agreement is valid until 2019.

In 2011 the European Commission resubmitted a 2007 proposal for an EU PNR Directive, which must provide for the transfer by airlines of PNR data of international flights to and from the Member States as well as the standardised processing of that data, which includes its receipt, use and retention by Member States and its sharing between them (EC, 2011a). For now it will not apply to intra-European flights; however Member States may opt to do so. The EU PNR Directive is focussed on supporting law enforcement agencies to anticipate and prevent terrorism and serious crime as well as making threat analyses of individuals on the basis of objective assessment criteria (EC, 2011a).

In addition to PNR information, more and more states are asking for API data. API data generally consist of the passenger manifest per flight, combined with passport information of each individual on board the concerning flight. The original goal was to increase passenger facilitation by reducing the throughput time of passengers at immigration as the data was already available before passengers arrived at the border facility of the concerning country. However, now API data is also used for pre-screening passengers before the flight arrives at the country of destination. The EU launched its API Directive in 2004 (CEU, 2004). Currently, not all EU member states have implemented it into their national legislation. API data is collected at the moment of check-in: Either at home (via internet), at the kiosk (self-service) or at the airport at a check-in desk (by an agent). Currently more states begin to use interactive API, which allows them to receive the required data at the moment of check-in and enables agents to directly determine whether or not the passenger is allowed to travel abroad.

3.2 Digital Financial Data: Storage, Processing and Transfer

During the last decade, the sharing, processing and transfer of financial data has been a controversial digital security governance issue in Europe. Even though US authorities had cooperated with authorities and companies located in Europe already directly after 9/11, it first became public in 2006 that digital financial data had been transferred to the Treasury Department and the Central Intelligence Agency (CIA) for counter-terrorism purposes. Only after US newspapers (Note 7) had reported about a confidential scheme, which allowed the US to monitor financial transactions made through the Society for Worldwide Interbank Financial Telecommunications (SWIFT), did the US and the EU in 2007 negotiate a public agreement, which in 2010 was replaced by the US-EU SWIFT agreement (Archick, 2012; CEU, 2010c/2007b). On the basis of this agreement, the TFTP uses SWIFT to collect digital personal data relevant for financial transactions, which includes the ‘amount transferred, bank account numbers, method of transfer, names of the parties, their addresses and telephone numbers, and information about the financial institutions involved in the transaction’ (Santolli, 2008).

Initially by using administrative subpoenas, American authorities accessed the SWIFT databases of a Belgium-based consortium of international banks (Archick, 2012; Connorton, 2007). In order to comply with these requests, SWIFT violated Belgian and European law. The Belgian Data Protection Authority and the Article 29 Working Party concluded that the TFTP was incompatible with the EU Data Protection Directive 95/46/EC (Article 29 Data Protection Working Party, 2006). Later, due to the 2007 US-EU agreement, this dilemma for SWIFT of violating European law became less of an issue (CEU, 2007b). However, due to changes in the SWIFT databases structure, a new agreement had to be negotiated in 2009 with the European Commission and approved by the EU Council as well as the European Parliament, which due to the Lisbon Treaty had received co-decision rights for international agreements.

What by then was publically known as the 'SWIFT Affair' culminated in February 2010 when the European Parliament rejected the new proposal for a US-EU TFTP agreement, which ‘guaranteed to United States security authorities continued access to European financial data held by […] SWIFT’ (De Goede, 2012, 214). Human rights concerns about the protection of EU citizens’ data and the right to a judicial remedy were the primary factors leading to the rejection of the agreement. Even prior to the European Parliament vote, the affair symbolised important concerns about European digital data security governance. Firstly, it was not anticipated that complete non-compliance by a private actor with EU legislation was possible and that sanctions would be virtually non-existent. Secondly, it shed light on ’the problematic loss of control of the protection once personal data have left European jurisdiction’ (Fuster, De Hert & Gutwirth, 2008). Thirdly, the affair highlighted the need to assess necessity and proportionality of ‘bulk data’ transfers of all European customers to US authorities (Archick, 2012). This last issue would be dealt with by creating a European TFTP system, which is currently

being discussed within the EU, and would only transfer extracted, and not bulk, financial data (EC, 2011b).

4. Ethical Dilemmas of Digital Security Governance

Security governance on the basis of (digital) personal data raises questions about what is morally right or wrong. The political decision to legislate the use, process and transfer of digital personal data for purposes of terrorism management per definition leads to ethical dilemmas. For example, should the financial or passenger data of all Europeans be collected? Should everybody be included or just those people who are pre-determined as a potential risk (scope, necessity)? Who determines what these risk factors are? Are they evidence-based? Are oversight mechanisms installed for the executive entity and its officials (digital data management) (Solove, 2011)? Should digital personal data be shared with third countries? And, if so, under what conditions? Are there side effects of such practices (Neyland, 2006)? Does digital personal information improve security governance? And if so, to what extent is this proportionate (for example, is a terrorism threat different from theft)? Are politicians and policymakers aware of the ethical implications of information and communication technology? Are citizens informed about how these systems operate (Neyland, 2006)? Can an individual, who is denied a service or access, seek redress, for instance when personal data is incorrect (access to information and the right to correction) (Regan & Johnson, 2012)? And if so, how (Gaugnin, Hempel & Ilten, 2011)? Should only individual security officials or also organisations be held accountable for mistakes (Gaugnin, Hempel & Ilten, 2011; Art. 29 Working Party, 2010)?

5. Accountability in Digital Security Governance

In the context of digital security governance, accountability is increasingly becoming an umbrella concept to deal with these aforementioned ethical dilemmas (Eijkman, 2012; Gaugnin *et al.*, 2012; Art. 29 Working Party, 2010; Centre for Information Policy and Leadership / Hunton & Williams LLP (CIPL), 2009; OECD, 1980). Because there are broader socio-political, legal and technological concerns connected to the use of information and communication technology for digital security governance, the concept should be understood in a holistic manner; as neither purely legal nor solely political. For instance, during the last decade, the saga of PNR negotiations between the US and the EU showed that the European Parliament (Note 8) held the EU Council accountable both legally – by appealing to the ECJ with regard to the 2004 time-limited agreement – as well as politically – by withholding their vote on the draft 2007 PNR agreement while requesting a global external PNR strategy from the European Commission (EC, 2010; ECJ, 2006). Furthermore, the 2012 US-EU PNR agreement contained several technological data security requirements, an inclusion that was explicitly requested by the European Parliament (EP, 2010; US-EU PNR Agreement, 2012). This demonstrates that security governance on the basis of digital personal data requires that the responsible (political) authority may be held accountable on different levels. Blind (2011, 4) distinguishes between 'accountability as the philosophy of government', which relates to honesty about the aforementioned socio-political, legal and technological considerations, and accountability as the 'means' of government, which concerns implementation.

In this analysis, accountability is conceptualised as a process: 'To be accountable, is to be in motion, not simply sitting in an office while being open to criticism' (Blind, 2011, 15). It is a dialogue, explanation and justification (Ackerman, 2005). In the context of accountability for digital security governance, one needs to differentiate between two distinct elements. On the one hand, there is the process by which, for example, EU institutions inform Europeans about terrorism risk management initiatives such as the US-EU TFTP agreement or the US-EU PNR agreement and justify the need to do so. On the other hand, the procedure under which the actual behaviour of public and/or private entities or security officials engaged in the implementation are subject to review or sanctions. From this perspective, accountability is partly characterised by mechanisms that are based on notions of the rule of law and good governance (Blind, 2011). It implies that those politically responsible (e.g., EU institutions or Member States) announce not only publically the purpose of digital personal data collection, processing, mining or sharing, but also limit its use to pre-defined threats such as in the case of financial data, which is meant to deal with terrorism (EP, 2012). One of the ways to guarantee this is designing responsible innovation, which may include privacy-enhancing-technologies (PETs) or transparency-enhancing-technologies (TETs) (Art.29 Working Party, 2010). (Note 9) For example, for the future EU TFTP programme this might entail that European authorities are able to authorise and monitor logging obligations.

Simultaneously, international and/or national law makers determine what the boundaries are for the international transfer of PNR or financial data, and how data subjects can seek redress through internal and/or or external accountability mechanisms. To illustrate this, in the renegotiated US-EU PNR Agreement, US authorities are required to give individuals more information and possibilities to seek redress for the use or processing of PNR data (Art. 11-13 US-EU PNR Agreement, 2012). Furthermore, the time of data retention has been reduced from

fifteen years to ten, whereas data connected to terrorism remains accessible for up to fifteen years. After six months of storage, the data is de-personalised and after five years it is transferred to a 'dormant database', where it is stored for up to ten years (Art. 8 US-EU PNR Agreement, 2012).

Nonetheless, despite these mechanisms, the crux of the issue in terms of ensuring accountability is in how it operates in practice (Art. 29 Working Party, 2010). What mechanisms ensure that the use or processing of digital personal data is adequately protected (Blind, 2011; Gaugnin *et al.*, 2012)? Can the semi-automatic actions by public and/or private entities or the responsible security officials be subject to adequate review or possibly even sanctions? One of the concerns with the 2012 US-EU PNR Agreement is that the options for redress are too limited (Note 10). National security interests, for instance, may too easily prevent the access of individuals to their digital personal data (Art. 11 US-EU PNR Agreement, 2012). With the 2010 US-EU SWIFT Agreement similar concerns are expressed by Members of the European Parliament (Archick, 2012).

6. Conclusion

The use of digital personal data for threat analysis has increasingly enhanced terrorism risk management. This article contributes to the discussion about accountability for storing, using, mining and transferring digital personal data. By focussing on passenger or financial data, it reviews some of the side effects of digital security governance in Europe. This is crucial because recent developments suggest that the use of information and communication technology in the fight against terrorism requires more political and public legitimacy. The Passenger Name Record (PNR), Advance Passenger Information (API) or Terrorist Finance Tracking System (TFTS) programmes, for instance, lead to questions about the necessity and proportionally of mass storage, use, mining and transferal of digital personal data to third countries.

Ethical dilemmas challenge public and private actors, who carry responsibility for storing, processing and transferring digital personal data. For example, the transfer of digital financial or travellers' data from Europe to the US may lead to data protection concerns. Continuous political and public debate about what accountability entails in the context of digital security governance is necessary. In this article, accountability has been understood as a process. This suggests that in addition to the rule of law and good governance, public and private authorities have to be aware and take responsibility for the side effects of digital security governance on the basis of personal data. These side effects may include violating the right to seek redress if the information is incorrect or the right to privacy when religious meal preferences are used as an indicator of a threat analysis for terrorism risk management. Even though this is more easily said than done, being accountable shows concerned citizens that ethical dilemmas such as the right to a judicial remedy can be dealt with in practice. This may contribute to long-term political and public legitimacy for digital security governance.

Acknowledgements

This article is based on the ICCT-the Hague seminar 'Digital Security Governance and Accountability in Europe', which was held on March 27, 2013 at Leiden University Campus the Hague in the Netherlands. The author would like to thank Sebastian Lenze and Nicolas Castellon for their assistance and Klaas Bruin for his feedback.

References

Ackerman. J. M. (2005). Social Accountability in the Public Sector: A conceptual discussion. In *Social Development Papers: Participation and Civic Engagement* (No. 82, p. 6). Retrieved February 23, 2013, from http://siteresources.worldbank.org/INTPCENG/214574111650607475 0/20542263/FINALAckerman.pdf

Archick, K. (2012). US-EU Cooperation against Terrorism. Congressional Research Service. Retrieved February 22, 2013, from http://www.fas.org/sgp/crs/row/RS22030.pdf

Art. 29 Working Party (Article 29 Data Protection Working Party). (2006). *Opinion 10/2006 on the Processing of Personal Data by the Worldwide Interbank Financial Telecommunication (SWIFT)*, Brussels: Article 29 Data Protection Working Party, November 22, 2006.

Art. 29 Working Party (Article 29 Data Protection Working Party). (2010). *Opinion 3/2010 on the Principle of Accountability*. Brussels: Article 29 Data Protection Working Party, July 13, 2010.

Balzacq, T. (2008). The Policy Tools of Securitization: Information exchange E.U. foreign and interior policies. *Journal of Common Market Studies, 46*(1), 78-82.

Blind, P. K. (2011). Accountability in Public Service Delivery: A multidisciplinary review of the concept. Expert Group Meeting Engaging Citizens to Enhance Public Sector Accountability and Prevent Corruption in the Delivery of Public Services, Vienna. Retrieved February 21, 2013, from

http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan046363.pdf

Borking, J. J. F. M. (2010). *Privacyrecht is een Code: Over het gebruik van Privacy Enhancing Technologies.* (Privacy is a Code: About the use of Privacy Enhancing Technologies), Kluwer: Deventer.

Ceccorulli, M., Fioramonti, L., Hanau Santini, R., & Lucarelli, S. (2010). *EU Security Governance.* EU-Grasp Working Paper, No. 2. Retrieved February 19, 2013, from http://www.eugrasp.eu/working-papers

Centre for Information Policy and Leadership / Hunton & Williams LLP. (CIPL) (2009). *Accountability: A compendium for stakeholders*. Centre for Information Policy and Leadership / Hunton Williams Llp. Retrieved February 20, 2013, from http://www.huntonfiles.com/files/webupload/CIPL_Centre_Accountability_Compendium.pdf

Centre for Information Policy and Leadership / Hunton & Williams LLP. (CIPL) (2011). *Accountability: Data governance for the evolving marketplace*, Centre for Information Policy and Leadership / Hunton Williams Llp. Retrieved February 22, 2013, from http://www.huntonfiles.com/files/webupload/CIPL_Centre_Accountability_Compendium.pdf

Council of the European Union (CEU). (1995). *Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data*. Council Doc. 1995/46/ EC, Brussels, October 24, 1995.

Council of the European Union (CEU). (2003). *The European Security Strategy for the European Union*. Brussels, December 12, 2003.

Council of the European Union (CEU). (2004). *Directive on the Obligation of Carriers to Communicate Passenger Data*. Council Doc. 2004/82/EC, Brussels, April 29, 2004.

Council of the European Union (CEU). (2005). *European Union Counter-Terrorism Strategy*. Council Doc.14469/4/05, Brussels, November 30, 2005.

Council of the European Union (CEU). (2007a). *Implementation of the Strategy and Action Plan to Combat Terrorism*. Brussels, Council Doc. 15411/1/07 Rev.1, Brussels, November 28, 2007.

Council of the European Union (CEU). (2007b). *Processing of EU Originating Personal Data by the United States Department of Treasury for Counter-Terrorism Purposes-'SWIFT'*. Official Journal of the European Union C/166/09, Brussels, July 20, 2007.

Council of the European Union (CEU). (2008). *Report on the Implementation of the European Security Strategy for the European Union - Providing Security in a Changing World.* Council Doc. S407/08, Brussels, December 11, 2008.

Council of the European Union (CEU). (2010a). *Internal Security Strategy for the European Union: Towards a European security model.* Council Doc. 5842/2/2010, Brussels, March 25, 2007.

Council of the European Union (CEU). (2010b). *The Stockholm Programme: An open and secure Europe serving and protecting citizens*. Official Journal of the European Union 2010/C 115/01, Brussels, May 4, 2010.

Council of the European Union (CEU). (2010c). *Agreement between the European Union and the United States of America on the Processing and Transfer of Financial Messenger Data from the European Union to the United States for the Purposes of the Terrorist Finance Tracking Programme*. Official Journal of the European Union 2010/L 195/05, Brussels, July 27, 2010.

Council of the European Union (CEU). (2011). *Agreement between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security*. Council Doc. 17434/11, Brussels, December 8, 2011.

Eijkman, Q. A. M. (2012). Counter-terrorism, Technology and Transparency: Reconsidering state accountability. *The Journal of International Security and Terrorism (IST), 3*(1), 29-40. Retrieved February 25, 2013, from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2199118

European Commission & High Representative of the European Union for Foreign Affairs and Security Policy (EU&HREU). (2013). *Cyber Security Strategy of the European Union: An open, safe and secure cyberspace*. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Joint 2013(1)final, Brussels, March 7, 2013.

European Commission (EC). (2010). *Communication from the Commission on the Global Approach to Transfers of Passenger Name Record (Data) to Third Countries*. COM(2010)0429, Brussels, September 21, 2010.

European Commission (EC). (2011a). *Proposal for a Directive on the European Parliament and of the Council on the Use of Passenger Name Record Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime*. COM(2011)32 final, 2011/0023 (COD), Brussels, February 2, 2011.

European Commission (EC). (2011b). *Communication from the European Commission to the European Parliament and the Council: A European finance tracking system: Available options*. COM(2011)429 final (COD), Brussels, July 13, 2011.

European Commission (EC). (2011c). *Commission Staff Working Document: Report of the joint review of the Agreement between the European Union and the United States of America on the Processing and Transfer of Financial Messenger Data from the European Union to the United States for the Purposes of the Terrorist Finance Tracking Programme*. COM(2011), Brussels, March 16, 2011.

European Commission (EC). (2012a). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century*. COM(2012) 9 final, Brussels, January 25, 2012.

European Commission (EC). (2012b). *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)*. COM(2012) 11 final, Brussels, January 25, 2012.

European Commission (EC). (2012c). *Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*. COM(2012) 10 final, Brussels, January 25, 2012.

European Commission (EC). (2012d). *Commission Staff Working Document: Report of the joint review of the Agreement between the European Union and the United States of America on the Processing and Transfer of Financial Messenger Data from the European Union to the United States for the Purposes of the Terrorist Finance Tracking Programme*. COM(2012)454 final (COD), Brussels, December 14, 2012.

European Court of Justice (ECJ). (2006). Judgement of the Court (Grand Chamber) of May 30, 2006, European Parliament v Council of the European Union (C-317/04) and Commission of the European Communities (c-318/04). Protection of Individuals with Regard to the Processing of Personal Data –Air Transport –Decision 2004/496/EC – Agreement between the European Community and the United States of America – Passenger Name Records of Air Passengers Transferred to the United States Bureau of Customs and Border Protection - Directive 95/46/EC – Article 25 – Third Counties – Decision 2004/535/ EC – Adequate Level of Protection, Nr.2006-I 04721.

European Parliament (EP). (2010). *Resolution on the Launch of Negotiations Passenger Name Records (PNR) Agreements with the United States, Australia and Canada*. Committee on Civil Liberties, Justice and Home Affairs, P7_TA (2010)0144, Brussels, May 5, 2010.

European Parliament (EP). (2012). *Recommendation on the Draft Council Decision on the Conclusion of the Agreement between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security*. Committee on Civil Liberties, Justice and Home Affairs, EP A7-0099/2012, Brussels, April 3, 2012.

Gaugnin, D., Hempel, L., & Ilten, C. (2011). Privacy Practices and the Claim for Accountability. In R. von Schomberg (Ed.), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields* (pp.100-114). European Commission: Brussels.

Gaugnin, D., Hempel, L., Ilten, C., Kroener, I., Neyland, D., & Postigo. (2012). *Managing Privacy through Accountability*. Palgrave/MacMillan: London. http://dx.doi.org/10.1057/9781137032225

Goede, M. de. (2008). The Politics of Preemption and the War on Terror in Europe. *European Journal of International Relations, 14*(1), 161-185. http://dx.doi.org/10.1177/1354066107087764

Goede, M. de. (2012). *Speculative Security: The politics of pursuing terrorist monies*. Minneapolis: University of Minnesota Press.

Hasbrouck, E. (2009). *What is in a Passenger Name Record (PNR)*. Website The Practical Nomad. Retrieved February 21, 2013, from http://hasbrouck.org/articles/PNR.html

Hegemann, H. (2012). *Between Great Transformation and Politics as Usual: Formal and informal security*

governance in EU counter-terrorism policy. Economics of Security Paper, No. 61. Retrieved February 20, 2013, from http://www.economics-of-security.eu/publications

Hildebrandt, M. (2011). Privacy Enhancing Technologies. *Hide Project, Pets 2nd Focus Group.* Retrieved February 20, 2013, from http://ebookbrowse.com/hide-fg-privacy-enhancing-technologies-minutes-20091016-pdf-d113363089

Hilty, L. M., Behrendt, S., Binswanger, M., Bruinink, A., Erdmann, L., Fröhlich, J., Köhler, A., Kuster, N., Som, C., & Würtenberger, F. (2005). *The Precautionary Principle in the Information Society: Effects of effusive computing on health and environment.* TA 46e/2005, TA-Swiss, Centre for Technology Assessment: Bern. Retrieved February 21, 2013, from http://www.ta-swiss.ch/incms_files/filebrowser/2005_46e_pervasingcomputing_e.pdf

House of Lords. (2007). The EU/US Passenger Name Record (PNR) Agreement. *Report with Evidence 21, European Union Committee.* London: The Stationary Office.

Jong, S. de, Sterkx, S., & Wouters, J. (2010). *The EU as Regional Actor: Terrorism.* EU-Grasp Working Paper, No.9. Retrieved February 19, 2013, from http://www.eugrasp.eu/working-papers

Kirchner, E. J. (2007). European Union: The European Security Strategy versus National Preferences. In E. J. Kirchner, & J. Sperling (Eds.), *Global Security Governance: Competing Perceptions of security in the 21st century* (pp. 113-134). Abingdon, New York.

Kirchner, E. J. (2007). Regional and Global Security: Changing threats and institutional responses. In E. J. Kirchner, & J. Sperling (Eds.), *Global Security Governance: Competing perceptions of security in the 21st century* (pp. 3-22). New York: Abingdon.

Knake. (2010). Untangling Attribution: Moving accountability in cyberspace. Council on Foreign Relations. Retrieved February 17, 2013, from http://science.house.gov/sites/republicans.science.house.gov/files/documents/hearings/071510_Knake.pdf

Müller-Wille, B. (2008). The Effect of International Terrorism on EU Intelligence Cooperation. *Journal of Common Market Studies, 46*(1), 49-73. http://dx.doi.org/10.1111/j.1468-5965.2007.00767.x

Neyland, D. (2006). *Privacy, Surveillance and Public Trust.* Palgrave/MacMillan: London. http://dx.doi.org/10.1057/9780230504561

Neyland, D. (2012). The Challenges of Working Out Surveillance and Accountability in Theory and in Practise. In D. Gaugnin, L. Hempel, C. Itlten, I. Kroener, D. Neyland, & H. Postigo (Eds.), *Managing Privacy through Accountability* (pp. 83-102). London: Palgrave/MacMillan.

O'Neill, M. (2012). *The Evolving EU Counter-Terrorism Legal Framework.* New York: Routledge.

O'Neill, M. (2013). *New Challenges for the EU Internal Security Strategy*. Newcastle upon Tyne: Cambridge Scholars.

Organization for Economic Development (OECD). (1980). *OECD Guidelines on the Protection of Privacy and Transborder Movement of Personal Data*, OECD. Retrieved February 19, 2013, from http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Papakonstantinou, V., & Hert, P., de. (2009). The PNR Agreement and Transatlantic Anti-Terrorism Cooperation: No Firm Human Rights Framework on Either Side of the Atlantic. *Common Market Law Review, 46*(3), 885-919.

Pawlak, P. (2007). From Hierarchy to Network: Transatlantic governance of Homeland Security. *Journal of Global Change and Governance, 1*(1), 1-22.

Regan, R., & Johnson. (2012). Privacy and Trust in Socio-Technical Systems of Accountability. In D. Gaugnin, L. Hempel, C. Itlten, I. Kroener, D. Neyland, & H. Postigo (Eds.), *Managing Privacy through Accountability* (pp. 125-142). Palgrave/MacMillan: London.

Schomberg, R. von. (2006). The Precautionary Principle and its Normative Challenges. In E. Fischer, J. Jones, & R. von Schomberg (Ed.), *Implementing the Precautionary Principle: Perspectives and prospects* (pp. 19-42). Edward Elger: Northampton. Ma, US / Cheltenham, UK.

Schomberg, R. von. (Ed.). (2011). *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields*. European Commission: Brussels.

Solove, D. J. (2011). *Nothing to Hide: The false tradeoff between privacy and security*. New Haven & London: Yale University Press.

Subrahmanian, V. S., Mannes, A., Silva, A. Shakarian, J., & Dickerson J. P. (2013). *Computational Analysis of Terrorist Groups: Lashkar-e-Taiba*. New York: Springer. http://dx.doi.org/10.1007/978-1-4614-4769-6

US-EU PNR Agreement. (2012). European Union - United States. "Agreement between the United States of American and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security." Council Decision 2012/472EU, 11 April 2012 and Council Decision 2012/472EU, December 13, 2011.

Valverde, M. (2003). Targeted Governance and the Problem of Desire. In R. Ericson, & A. Doyle (Eds.), *Risk and Mortality* (pp. 238-250). Toronto: University of Toronto Press.

Valverde, M., & Mopas, M. S. (2004). Insecurity and the Dream of Targeted Governance. In W. Larner, & W.Walters (Eds.), *Global Governmentality* (pp. 233-251). New York: Routledge.

Vermeulen, M., & Bellanova, R. (2012). European 'Smart' Surveillance: What's at stake for data protection, privacy and non-discrimination? *Journal of Security and Law, 4,* 297-311.

Vries, de, G. (2005). The European Union's Role in the Fight against Terrorism. *Irish Studies in International Affairs, 16*, 3-9

Webber, M. (2004). The Governance of European Security. *Review of International Studies, 30*(3), 3-26.

Wright, D. (2010). Sorting out Smart Surveillance. *Computer Law & Security Review, 26*(4), 347. http://dx.doi.org/10.1016/j.clsr.2010.05.007

Wright, D., & Hert, P. de. (Eds.). (2012). *Privacy Impact Assessment*. Dordrecht: Springer. http://dx.doi.org/10.1007/978-94-007-2543-0

Wright, D., Gellert, R., Gutwirth, & Friedewald, M. (2011). Precaution and Privacy Impact Assessment as Modes Towards Risk Governance. In R. von Schomberg (Ed.), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields* (pp. 84-97). European Commission: Brussels.

Notes

Note 1. This definition is partly based on the concept of 'targeted governance', which Valverde (2003, 438), defines as "governing security and safety through risk techniques that identify and evaluate the presence and the magnitude of risk factors in people, spaces, and activities is connected to - and is sometimes just a part of - a very generalized way of governing….." See also Valerda & Mopas (2004, 245).

Note 2. The full definition of cyber security, which is not officially recognised within the EU (EU&HREU, 2013, 3) "Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein."

Note 3. In January 2012 two drastic legislative proposals and a communication about revising data protection legislation by private and public actors were issued by the European Commission (European Commission (EC) , 2012a/b/c).

Note 4. See among others: Schomberg, 2011 and also several FP7 projects including the Detecting Technologies, Terrorism, Ethics and Human Rights ('DETECTER'), 2008-2011 see http://www.detecter.eu/ the Project Privacy Awareness Through Security Organization Branding ('Pats Project'), 2010-2013, see www.pats-project.eu the Project Building International Cooperation for Trustworthy ICT: Security, Privacy and Trust in Global Networks and Services ('BIC-Trust'), 2011-2013, see http://www.bic-trust.eu the Project Surveillance: Ethical issues, Legal Limitations and Efficiency ('SURVEILLE'), 2012-2014, http://www.surveille.eu; the Project Scalable Measures for Automated Recognition Technologies ('SMART'), 2011-2014, see http://www.smartsurveillance.eu the Project Privacy and Security Mirrors ('PRISMS'), 2012-2015, see http://prismsproject.eu.

Note 5. Among others the Eurodac (biometric database for the identification of asylum seekers), EC/CEU Regulation (EC) 2725/2000,11 December 2000 / ECRIS system (enabling EU countries to access each other's national criminal records) / the Schengen Information System I (SIS II will replace SIS I, Council of the European Union Decision 2007/533/JHA,12 June 2007 and Regulation (EC) 1987/2006, 20 December 2006)

contains data on aliens who have been declared 'undesirable', but is primarily intended for tracking down suspects and convicted criminals..

Note 6. Even though the EU has similar agreements with other states including Canada and Australia, the US-EU Agreement is focussed upon in this article.

Note 7. New York Times, Los Angeles Times, Wall Street Journal, Washington Post.

Note 8. Since the Lisbon Treaty in 2009 was ratified the European Parliament has the co-decision right in relation to international agreements.

Note 9. See among others the FP7 Project Privacy Awareness Through Security Organisation Branding (www.pats-project.eu).

Note 10. This is one of the reasons why two Member States, Germany and Austria, abstained from voting about the 2012 US–EU PNR Agreement (Archick, 2012).