SECURITY, TECHNOLOGY AND ACCOUNTABILITY: REASSESSING THE ROLE OF THE STATE?

Güvenlik, Teknoloji ve Hesap Verebilirlik: Devletin Rolünün Yeniden Değerlendirilmesi

Quirine Eijkman*

Abstract

This article discusses the use of surveillance, storage of personal information, biometrics, satellite technology and other forms of ICT technology for security purposes. Although technology is a powerful tool to fight terrorism, it is also a means for increasing social control by the state. Henceforth, there is a risk that panoptic surveillance, where the few view the many, could develop. In this context the role of the state, because of its monopoly to use force and its duty to protect the rule of law, is crucial. Henceforth, by reassessing state accountability, the impact of technological security measures may be checked and balanced.

Keywords: Accountability, Technology, Security, Rule of law, Surveillance, counter-terrorism

Özet

Bu makale gözetim, kişisel bilgilerin depolanması, biyometri, uydu teknolojisi ve ICT teknolojisinin diğer biçimlerinin güvenlik amaçlarıyla kullanılmasını tartışır. Teknoloji terörizmle mücadelede güçlü bir araç olmasına rağmen aynı zamanda devletin sosyal kontrolü artırması içinde bir araçtır. Zira, az sayıdaki görevlinin toplumu izlemesi anlamında panoptic gözetlemeye dönüşme riski bulunmaktadır. Bu bağlamda, devletin rolü, onun zor kullanmada ve hukuk kurallarını koruma görevinde tekel olmasından dolayı hayatidir. Zira, devletin hesap verebilirliği yeniden değerlendirilerek teknolojik güvenlik önlemlerinin etkisi kontrol edilebilir ve dengelenebilir.

Anahtar Kelimeler: Hesap verebilirlik, Teknoloji, Güvenlik, Hukuk kuralı, Gözetleme, Terörle mücadele

* *Dr. Quirine Eijkman is a Senior Researcher and Lecturer at the Centre for Terrorism and Counterterrorism at Leiden University – Campus the Hague and a Research Fellow at ICCT-The Hague, the Netherlands. The author would like to thank Ms. Orla Hennessy and Mr. Daan Weggemans for their assistance.*

Introduction

In the fight against terrorism technology is a powerful tool. As the European Group of Personalities in the field of Security stated "technology itself cannot guarantee security, but security without the support of technology is impossible" (European Communities, 2004, p.12). This quote illustrates how information and communications technology (ICT), biotechnology, neuroscience and nanotechnology contribute to the development of important security strategies. It also reminds us that we should be realistic about the impact of technological counter-terrorism measures. There are, for example, no quick solutions to deal with the threat of terrorism. Osama bin Laden, for instance, was found on the basis of human intelligence. Only after his possible location in Abbotabad in Pakistan was traced, did technology including satellite surveillance, Forward Looking Infrared Devices (FLIR) and biometric Secure Electronic Enrolment Kits (SEEKs) play a role in detecting activity in the compound and in identifying the Al Qaeda leader (English, 2011).

Increasing contemporary security concerns such as international terrorism seem to justify the use of innovative technological tools. After all, terrorists draw on modern technology, especially the internet (Fenwick, 2011; European Council 2009). Cyber-attacks on critical infrastructure such as energy or communication networks, state computer-networks etc., lead to new complex national security threats. Thus, by using technological security tools the state is simply adjusting to contemporary societal developments. However, what distinguishes the state from others such as private entities is their monopoly on the use of force and its protection of the rule of law. Additionally, security technologies are a potential powerful means of social control by the state and there are foreseen and unforeseen social consequences to their use (Bruggeman, 2011). If there are, for instance, no proper checks and balances in relation to new technological counter-terrorism tools, there is a risk that, to quote Mathiesen (1997) 'panoptic'[1] surveillance develops: Where the few, in this case the state, continuously keep under observation the many, the people (Cohen, 1995; Foucault, 1979). This facilitates the creation of a so-called 'surveillance society'[2], where the collection of personal data affects everybody, potential terrorists as well as ordinary people who run the risk of being (preventively) labelled a threat to national security or public order.

In the context of the increased use of new technology for security purposes a key question remains if technological security measures should lead to reassessing state accountability? Do new technologies, for instance, lower the threshold for the state to socially control society? And could they affect compliance with the rule of law? In this article, the concept of accountability is discussed. Subsequently, technological security measures are outlined, followed by a discussion on the effect these new tools may have on state accountability. The concluding section reflects upon the question whether or not the use of new technologies for security purposes such as the fight against terrorism could lead to reassessing governmental accountability.

[1] *He developed Foucault's use of Bentham's concept of 'Panopticon' (1979) and Cohen (1995).*

[2] *"Surveillance societies "function, in part, because of the extensive collection, recoding, storage, analysis and application of information and individuals and groups in these societies as they go about their lives" (Surveillance Studies Network, 2010). See also Wood and Webster, 2009 and Lyon, 2007.*

1. The Concept of Accountability

New technological developments have increased the range of security tools at the disposal of policymakers and security and intelligence officials. While many counter-terrorism laws, policies and programmes that structure and regulate the use of these new technologies recognize the importance of the rule of law and human rights in, civil society continues to focus on concepts that tend to show a certain cross-cutting relationship: How can terrorism be countered effectively whilst ensuring accountability (Neyroud and Disley, 2008, Liberty, 2007? Thus, with the emergence of new security technologies, a common concern has developed with respect to state accountability.

The concept of accountability entails two distinct features. On one hand, there is a strong normative aspect intertwined with notions of justice, responsibility, integrity, fairness and democracy (Blind, 2011). At the same time, the definition of accountability is concrete and 'value free' while it focuses on the 'obligations to evidence management or performance imposed by law, agreement or regulation' (Kohler, 1975, p.6). Accountability therefore can be described both in terms of a virtue and as a mechanism through which a certain actor, in this case, a state, can be held to account by a forum or civil society group (Pollitt, 2003, p.3). Blind classifies this distinction in terms of 'accountability as the philosophy of government' and accountability as the 'means' of government (Blind, 2011, p.4).

In this article, Ackermans's definition (2005, p.6) of government accountability is used, which views the concept as a process where representatives of the state, public officials, inform society about their plans and actions and justify them simultaneously, while their actual behavior and results are subject to sanctions accordingly. This form of accountability is characterised by its focus on the rule of law and good governance as well as the inclusion of civil society and ordinary people (Blind, 2011; Ackerman, 2005). Thus, in addition to political accountability, for example, through elections, it is enforced by advocacy campaigns, investigative journalism or audit commissions.

2. Technological Security Measures

New technologies have enlarged the range of available possibilities to protect security for policymakers and security and intelligence agencies. The actual deployment of new technological security measures is often initiated by politicians who, due to real or perceived threats, are pressured by a large part of society to 'do something' about terrorism (Graaf, 2011, Cole 2004). In particular, security and intelligence agencies increasingly use surveillance technologies to gather (soft) intelligence about individuals and groups. This, however, does not happen in a vacuum, technological trends affect society at large. Many new technologies such as the internet and Global Positioning System (GPS) have dual purposes (GOP, 2004). They may have been designed for the military, but also support law enforcement as well as commercial activities. Moreover, they serve both the general public and are at the same time used by terrorist organizations

Without providing an exhaustive list of technological security measures, a few 'new' technologies are discussed in this section. They include biometrics, visual surveillance and the tracing of personal data. These three examples have been selected because of the increased interest authorities express in digital personal data, the visibility of the particular measure and/or people's own experiences with it. They are therefore assumed to influence public debate about new technologies in relation to the fight against terrorism. Henceforth, these examples will serve as a basis for the discussion about state accountability.

2.1. Biometrics

Biometric devices and databases are used to collect and store large amounts of data on individuals' physical characteristics. The personal information recorded and stored can include digital images of faces, fingerprints, palm patterns, iris scans, DNA, vehicle registration, insurance information, criminal records and possibly even speech patterns, scars, and the distinct way in which people walk. Coupled with 'smart' surveillance or recognition technology such as Closed Circuit Television [CCTV] systems capable of matching information in the database against real-time images, biometric databases greatly increase governments' ability to monitor their citizens (Bowcott, 2008; Taslitz, 2002).

One of the concerns in relation to biometric databases is that they are contributing to a trend in state surveillance whereby people are kept under constant observation without any prior indications of involvement in criminal activities or disorderly behaviour. Furthermore, people are usually not aware of being observed or which authority is responsible for the surveillance. Additionally, the frequent storage of inaccurate personal data and the often limited possibilities of correcting such information makes it problematic to hold the state accountable (Council of Europe, 2007). As biometric data does have error margins, for example in relation to fingerprints, this is a cause for concern: Innocent individuals could be incorrectly 'flagged' as potential terror suspects (false-positive results) and subjected to further, unwarranted, investigation (Böhre, 2010).

There are several specific concerns in relation to the use of biometrics by security and intelligence agencies. The use of biometrics, for instance, poses a threat to right to privacy. The question is to what extent the increased ability to detect and arrest suspects outweighs this significant drawback. Other human rights concerns relate to the right to a fair trial, the right to personal data protection as well as the lack of proper oversight. For instance, citizens or foreign nationals could be inaccurately judged as suspects for a long period of time and thereby the presumption of innocence is under pressure. Also there is a risk that such databases could be the targets of cyber criminals, which may result in the abuse of sensitive personal information such as iris scans. Furthermore, the international linking of national biometric databases poses questions about transparency (what is being shared?), personal data protection and accuracy (data losses or fraud), and privacy (why should a foreign government have access to large amounts of sensitive information about foreign nationals?).

2.2. Visual Surveillance

Visual surveillance has become an important measure to counter terrorism (Fenwick, 2011; Eijkman and Weggemans, 2011). Surveillance technology, for instance, is used for gathering (soft) intelligence about individuals and groups. The core of the surveillance camera system is formed by a process in which video cameras collect images which in turn are transferred to a monitor from which they can be watched and recorded. Subsequently, the possessor of the system can decide to review and store the recorded images. Nowadays technical trends such as biometric and recognition technologies are emerging, which in addition to visual surveillance have data integration capabilities including data mining and profiling techniques. For instance, Automatic Number Plate Recognition (ANPR) systems are able to distil license plate information from camera images, processing these images either on the spot (i.e. in a police car) or by sending it to a large-scale computer facility. Once the license information has been extracted from the image, it is compared with various databases to verify whether or not the vehicle or its owner is sought by the authorities.

Initially, visual surveillance was predominantly used by retailers. Since then the system has evolved and now it is also used for countering terrorism. However, technological developments have led to the present day visual surveillance systems that are also used for countering terrorism; systems that are diverse and are accounted for differently. For example, Homburg and Schreijenberg (2010, pp.10-11) conclude that most Dutch municipalities record CCTV images (86 percent), but significant differences exist in the time span they are actually recording. Similarly, the way in which the images are recorded and viewed turned out to vary, as well as the storage and sharing (e.g. with intelligence services) of the captured material. Furthermore, the installation of surveillance cameras is usually a joint public-private affair. Public space surveillance measures are often financed by several parties, the state as well as private parties, but sometimes also by counter-terrorism funds. Finally, the people in the control room differ depending on their employer (police, private enterprises or government). Hence, even without directly focusing on the underlying legal matters, visual surveillance as part of a wider terrorism prevention strategy clearly is a complicated matter.

Although there is nothing inherently unlawful about the use of visual surveillance by the state, it can affect human rights (Council of Europe's Venice Commission, 2007; Justice, 2007). This may include infringements to the right to privacy, data protection, the freedom of movement and the freedom of association. Additionally, it may disturb some of the presumptions that underpin the relationship between the individual and the state. Choudhury, Tufyal and Fenwick (2011) evaluated the effects of surveillance cameras, funded by counter-terrorism funds, on Muslim majority communities in Birmingham and concluded that the deployment of surveillance measures can have a serious impact on the relationship between (local) authorities such as the police and (minority) communities. The use of surveillance cameras can lead members of the populations to doubt the legitimacy of the visual surveillance measures which eventually could result in 'significant community anger and loss of trust' (Choudhury, Tufyal and Fenwick, 2011, p.36). Hence, visual surveillance and recognition technology may indeed be important tools to counter terrorism, but (un) foreseen consequences could affect political and public debate about their use.

2.3. Tracking of Personal Data

In order to ensure security, personal information, such as biometric data or camera images, is not only collected and retained, but increasingly also processed, disseminated and shared between governmental agencies and sometimes third states. Public authorities become so-called information-Governments (i-Governments)[3] that employ data collection, retention, mining and cross-sharing techniques to minimise all major and minor risks to society. The European Union's and its Member States' counter-terrorism policies, for example, rely partly on the tracking of personal data such as the Passenger Name Record (PNR) system

[3] *The concept of i-Government implies that the government by using information and communication technologies (ICT) has become an independent actor in the information society and therefore the concept of e-Government, which usually only refers to the use of ICT, is no longer sufficient (Prins 2011, Mayer-Schönberger and Lazer 2007).*

(European Parliament 2011, European Council 2009). Furthermore, states use information technology to analyse personal data about individuals and groups who potentially could pose a threat to national security. This development is sometimes referred to as investing in the dream of 'targeted governance' (Valerda and Mopas 2004); promising to deploy systems that are tailored to predict and pre-empt terrorist acts and concentrate intelligence on a few targets. Such targeted technologies to fight terrorism include the terrorist finance tracking systems (e.g. TFTP , the US Foreign Assets Control [OFAC]) , the foreign nationals' databases and surveillance programmes (e.g. the EU Schengen Information System [SIS] and the USA Foreign Intelligence Services Act [FISAA]).

While governments frequently claim that an expansion of the powers to analyse personal information is necessary if police forces and security services are to maintain their capabilities vis-à-vis the fast pace of developments in ICT, such surveillance can pose a threat to citizens. As the following example suggests, information analysis by public authorities is vulnerable to unnecessary requests and poor enforcement of safeguards. In 2009, the Dutch Data Protection Authority concluded that the National Criminal Investigation Services violated criteria such as access to authorization set by special Acts[4] in their applications to the Central Information Point for Telecommunications Investigation, which was created in order to streamline information requests by the authorities to Internet and Telecom companies (Data Protection Authority, 2011).[5]

Furthermore, there is a noticeable trend in the United States of America (USA) whereby police and security services' powers of electronic surveillance have been incrementally expanded since the late 1980s. The 2001 Patriot Act exemplifies how 'national security' is often touted as the reason why increased surveillance authority is required, even if it compromises citizens' private lives. Furthermore, many American data mining programmes are covert and lack transparency: People are unaware that their personal information is given by third parties to the state, oversight is lacking and the ability to correct errors is limited (Solove 2008, 2004). While the main concern in relation to the tracking of personal data is in the USA, in the EU as well as in other states, is a profound intrusion into persons' privacy, there are also concerns about data protection, non-discrimination and lack of oversight, transparency and accountability (EPDS, 2011; Bloss, 2009; Allen, 2008; Clayton, 2006).

3. Reassessing State Accountability?

Thus although public authorities draw on new technologies for security purposes, their increased interest in these tools raises questions about their social repercussions. These concerns are partly addressed by focussing on the checks and balances, which implies that the state is held accountable for its laws, regulations, policies and actions and public officials are sanctioned accordingly. This also applies to the state's responsibility to supervise private entities. But what are the challenges of the process of governmental accountability in relation to technological security measures? If counter-terrorism technologies have enabled states

[4] *More specifically article 13 of the Personal Data Protection Act (WBP). The EU Privacy Directive is implemented in the WBP, Bulletin of Acts and Decrees 2000, 302, 1 September 2001; Articles 3(1/2), 4(3), 6(1) and 31(1c) of the Data Protection (Police Files) Act, 1 January 2008; Article 5(1) Telecommunications (Provisions of Information) Degree, 26 January 2000.*

[5] *In 2009 there were 2,9 Million requests by authorized authorities (Data Protection Authority, 2011, p.3).*

to become too powerful when enforcing the law and maintaining social control, to the extent that one risks the creation of panoptic surveillance, one wonders whether this development has affected discussion about the accountability of the state.

On the international level, the former United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terror, Martin Scheinin, has highlighted the erosion of the rights to privacy and data protection as well as function creep in relation to the fight against terrorism. According to Scheinin (UN Human Rights Council, 2009, p.14 and pp.22-27) the increased use of surveillance powers in places and on large groups of people leads to weaker systems of authorisation and oversight and technologies lack adequate legal safeguards. In relation to this call for more governmental accountability, the Special Rapporteur stressed the need for states to communicate in depth how the principles of necessity and proportionality are upheld in their surveillance policies and emphasised that independent and effective oversight for information based-technologies and more research about privacy enhancing technologies is required (UN Human Rights Council, 2009, p.14 and pp.33-34). Hence, in order to improve a state's accountability for technological counter-terrorism measures, the need for improved information about their impact, for strengthening oversight and research into technological solutions (privacy enhancing technologies) is crucial.

States with a long history in countering terrorism (like the United Kingdom (UK)) have gradually developed legal frameworks of accountability. Unfortunately, the rapid development and deployment of new technologies in this field in combination with its rigid character have led to parts of this framework becoming outdated or incomplete. Other countries with less experience with the use of (modern) technologies in fighting terrorism have usually developed modest systems of state accountability. In the UK, civil society organizations such as Liberty highlighted the increased usage of new technologies while 'data protection laws have become outdated and fail to keep pace with the reality of modern data processing' (Kitchin, 2007, p.1). This lack of accountability and transparency is also endorsed by human rights organization Justice, which has argued that despite the growth of new technology use in countering terrorism, these is no single legal framework governing this use. Where some parts are governed by the Data Protection Act, the regulation of placement and usage of surveillance cameras has remained, from a legal perspective, underexposed, e.g. with respect to personal data protection (Justice, 2007). The UK Home Office responded to criticism by planning to install two new commissioners and a code of practice for the use of open space surveillance cameras and biometrics by public authorities (House of Commons, 2011).

Furthermore, 'panoptic' surveillance by the state is simultaneously counter-balanced by the process of 'synopticism', as put forward by Mathiesen (1997, pp.218-219), where in the so-called 'viewer society' the many observe the few. New technologies including social media enable the public at large to become citizen journalists and subsequently to play a role in challenging institutional versions of events that have taken place (McLaughlin and Greer, 2010; Cottle, 2008). From this perspective, some kind of informal external accountability is established. Therefore civil society advocates should also focus on external accountability such as social media and advocacy reports, which in addition to existing internal accountability structures, function preventatively, randomly and transparently. Henceforth as the discussion about governmental accountability in relation to technological secures measures contents, one can raise the question whether state accountability should be reassessed. On one hand, when governmental accountability is emphasised, there are more opportunities for increased human rights protection and subsequently public legitimacy of, for example, the police and their use of 'new' technologies in the fight against terrorism (Neyroud and Disley, 2008). On the other hand, in the context of national security is not realistic to expect politicians, public officials and security officials to be completely transparent about security concerns. The exceptionality of the terrorist threat argument will often justify covert extraordinary measures (Zedner, 2007).

Nonetheless, security technologies such as smart surveillance cameras, biometric devices or the tracking of personal data that affect society at large should be justified not only on the basis of the human rights criteria of necessity, proportionality and effectiveness, but also in terms of their (long-term) public legitimacy. Are the new measures in accordance with the rule of law and popularly accepted? This should be assessed periodically and contextually; the impact of smart cameras on the right to privacy differs from that of DNA databases (Solove, 2010). Additionally, impact assessment, privacy by design, the transparency in the data flows and public awareness about how security technologies function should be improved (Wright and de Hert, 2012; EDPS, 2011; Graaf and Eijkman, 2011). This is necessary, as the political and public debate about the effect of security technologies on the diminishing of terrorist threats should be well-informed. The state then has a responsibility to communicate to and educate its citizens objectively about the content of security technology and its impact. Finally, when government agencies engage in data collection, retention, mining and cross-sharing, it must be transparent and clear to the institutions and public officials involved which agency is responsible for the information and that the outcome is subject to review, and if necessary sanctioned (EPDS, 2011).

Conclusion

With the emergence of technologies that enhance security, concerns have arisen in relation to states accountability. New technologies have enlarged the range of available possibilities for the state to protect national security. Many people are, however, unaware of the side-effects of for example technological counter-terrorism measures. These concerns are partly addressed by focusing on the checks and balances, which implies that public authorities are held accountable for their laws, regulations, policies and actions and are sanctioned accordingly. This also applies to a state's responsibility to supervise private entities. Thus the use of new (surveillance) technologies for security purposes raises questions about public legitimacy.

Overall the 'new' technologies that were discussed here are considered to be useful security tools. However, at the same time biometrics, visual surveillance and data analysis may lead to uncontrolled surveillance and affect human rights compliance. Their use by state officials can both in depth and breadth affect the rule of law significantly. This risk might be balanced by reassessing how to enforce state accountability. For instance, more transparency about data flows and impact assessments could raise public awareness about security technologies and their side-effects. Without proper checks and balances for the use of technological security tools, there is a risk that 'panoptic' surveillance, where a small minority of state officials or private security officials view the majority, the citizens, becomes pervasive.

References

Ackerman, J.M. (2005). ‘Social Accountability in the Public Sector: A conceptual discussion’, *Social Development Papers*: *Participation and Civic Engagement,* 82 March, 2005. Retrieved on 16-06- 2011 from http://siteresources.worldbank.org/INTPCENG/214574-1116506074750/20542263/FINALAckerman.pdf.

Allen, N. (2008, October 5). ‘Government Spies Could Scan Every Call, Text and Email’. *The Telegraph,* Retrieved on 20-1-2011 from http://www.telegraph.co.uk/news/uknews/law-and-order/3140207/Government-spies-could-scan-every-call-text-and-email.html.

Ashworth, A. (2007). *“Security, Terrorism and the Value of Human Rights”* (pp.203-225). In: Goold, B.and Lazarus, L. (Eds.), *Security and Human Rights*, Oxford: Hart Publishing.

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, Austria 1-8 & 11-13 July 2011. Retrieved on 21-07-2011 from http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan046363.pdf.

Bloss, W.P. (2009). ‘Transforming US Police Surveillance in a New Privacy Paradigm’. *Police Practice & Research,* Vol.10, nr. 3, pp. 225-238.

Böhre, V. (2010). *Happy Landings: Het biometrische paspoort als zwarte doos* [The biometric passport a black box], nr.46, The Hague: Scientific Council for Government Policy.

Bruggeman, W. (2011). “The Boundaries and the Future of Technological Control: Technological control has its limits on ethical ground, but also from a social controlpoint of view” (pp. 125-163), In: Pauw, E. de, Ponsaers, P. and Vijver, K. van der (Eds.), *Technological-Led Policing*, Cahier Politiestudies, 2011-nr.3, Antwerpen/Apeldoorn/Portland: Maklu Uitgevers.

Choudhury, Tufyal and Fenwick, H. (2011). The Impact of Counter-terrorism Measures on Muslim Communities, *Equality and Human Rights Commission Research Report Series*, nr. 72: Manchester: Equality and Human Rights Commission.

Clayton, M. (2006, February 9). “US Plans Massive Data Sweep”. *The Christian Science Monitor.* Retrieved on 20-1-2011 from http://www.csmonitor.com/2006/0209/p01s02-uspo.html

Cohen, S. (1985). *Vision of Social Control: Crime, punishment and classification,* Cambridge:Polity Press.

Cole, D. (2004). ‘The priority of morality: The emergency constitution’s blind spot’, *Yale Law Journal,* Vol.113, nr.7, pp. 1753-1800.

Cottle, S. (2008). ‘Reporting Demonstrations: The changing media politics of dissent’, *Media, Culture and Society*, Vol. 30, pp. 853-872.

Council of Europe (COE) (2007). *Recommendation of the Committee of Ministers to member states on measures to promote the public service values of Internet,* Council of Europe CM/ Rec. 16, 7.

Crossman, C., Kitchin, K., Kuna, R., Skrein, M. and Russell, J. (2007). Overlooked: *Surveillance and personal privacy in modern Britain,* London: Liberty.

Data Protection Authority (2011, April 21). *Onderzoek Dienst Nationale Recherche* [Research National Criminal Investigation Services], Decision Z2010-00170, The Hague: Data Protection Authority.

Eijkman, Q. (2011). "Police Technology and Human Rights: A quest for accountability" (pp.193-204), In: Pauw, E. de, Ponsaers, P. and Vijver, K. van der (Eds.), *Technological-Led Policing,* Cahier Politiestudies , 2011-nr.3, Antwerpen/Apeldoorn/Portland: Maklu Uitgevers.

English, M. (2011, May 3). 'Tech helped Nab and Identify Osama bin Laden', *Discovery News.* Retrieved 2-5-2011 from http://news.discovery.com/tech/osama-bin-laden-capture-technology-110503.html.

European Council (2009). 'The Stockholm Programme: An open and secure Europe servingand protecting citizens', *Official Journal of the European Union* (Publication 14449/09) Retrieved on 4-6-2010 from http://register.consilium.europa.eu/pdf/en/09/st14/st14449.en09.pdf.

European Data Protection Supervisor (2011). 'Counter-terrorism Policy and Data Protection',*Hearing of the European Economic and Social Committee*, 9 February 2011. Retrieved on 28-11-2011 from http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2011/11-02-09_Counter_terrorism_EN.pdf

European Parliament Committee on Civil Liberties, Justice and Home Affairs (2011). T*he EU Counter-Terrorism Policy: Main Achievements and Future Challenges,* A7- 0268/2011Draft Report of 20 July 2011, Retrieved from http://ec.europa.eu/commission_20102014/malmstrom/archive/Communication%20Counter%20Terrorism%20EN.pdf

Fenwick, H (2011). 'Counter-Terror Strategies, Human Rights and the Role of Technologies', *International Review of Law Computers and Technology*, Vol.25, nr.2, pp. 107-115.

Foucault, M. (1979). *Discipline and Punish: The birth of the prison*, New York: Vintage.

Graaf, B., de (2011). *Evaluating Counterterrorist Performance: A comparative study,* Abingdon: Routledge/Francis & Taylor.

Graaf, B., de and Eijkman, Q. (2011). 'Terrorismebestrijding en Securitisering; Een rechtssociologische verkenning van de neveneffecten' [Counterterrorism and Securitization: A social-scientist view on transparency and accountability of the side-effects], *Justitiële Verkenningen*, Vol.37, no.8, pp.33-53

Greer, C. and McLaughlin, E. (2010). 'We Can Predict a Riot? Public order policing, new media environments and the rise of the citizen journalist', *British Journal of Criminology*, Vol.50, nr.6, pp. 1041-1059.

European Communities (2004). '*Research for a Secure Europe*', Group of Personalities in the field of Security Research, Luxembourg: Office for Official Publications of European Communities. Retrieved on 22-11-2011 from http://www.src09.se/upload/External%20Documents/gop_en.pdf

House of Commons (2011). 'Protection of Freedoms Bill'. Retrieved on 04-07-2011 from http://www.publications.parliament.uk/pa/cm201011/cmbills/146/11146.20-26.html.

Kitchin, H. (2007). "Visual Surveillance" (pp.35-48), In: Crossman, G., Kitchin, H., Kuna, R., Skrein, M, Russell, J. (Eds). *Overlooked: Visual surveillance and personal privacy in* *modern Britain,* London: Liberty, pp. 35-47.

Kohler, E.L. (1975). *A Dictionary for Accountants, Englewood Cliffs* (N.J): Prentince Hall. Lyon, D. (2007). *Surveillance Studies: An overview*. Cambridge: Polity Press.

Mathiesen, T. (1997). 'The Viewer Society: Michel Foucault's Panopticon' revisited', *Theoretical Criminology*, Vol.1, nr.2, pp. 215-234.

Morozov, E. (2010). *The Net Revolution: How not to liberate the world,* London: Allan Lane.

Neyroud, P. and Disley, E. (2008). 'Technology and Policing: Implications for fairness and Legitimacy', *Policing,* Vol.2, nr.2, pp. 226-232.

Osse, A. (2006). *Understanding Policing:* A resource book for human rights activists. Amsterdam: Amnesty International Dutch Section.

Prins, C. (2011). *Overheid* [The Information-Government], nr. 86, The Hague: Scientific Council for Government Policy.

Pollitt, C. (2003). *The Essential Public Manager,* London: Open University Press/McGraw.

Schreijenberg, A. and Homburg, G.H.J. (2010). *Steeds meer Beeld: Evaluatie vijf jaar cameratoezicht op openbare plaatsen* [Increasingly More Policy: Evaluation of five years of camera supervision]. Retrieved on 22-06-2011 from http://www.hetccv.nl/instrumenten/Cameratoezicht-publiek/landelijk---steeds-meer-beeld

Solove, D.J. (2004). *The Digital Person: Technology and privacy in the information age,* New York: New York University Press.

Solove, D.J. (2007). *Understanding Privacy*, Cambridge: Harvard University Press.

Surveillance Studies Network (SSN) (2010). *An Introduction to the Surveillance Society.* Retrieved on 17-1-2011 from http://www.surveillance-studies.net/?page_id=119

Stone, C. E., and Ward, H. H. (2000). 'Democratic Policing: a Framework for Action'. *Policing and Society*, Vol. 10, nr.1, pp. 11-45.

Taslitz, A.E. (2002). 'The Fourth-Amendment in the Twenty-First Century: Technology, privacy, and human emotions', *Law and Contemporary Problems,* Vol.65, nr.2, pp. 125-127.

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

UN Human Rights Council (2009). Promotion and Protection of Human Rights, Civil, *Political, Economic, Social and Cultural Rights, Including the Right to Development and Fundamental Freedoms While Countering Terrorism, Geneva:* Human Rights Council, A/HRC/37, 28 December 2009. Retrieved on 03-07-2011 from http://www2.ohchr.org/english/issues/terrorism/rapporteur/docs/A_HRC_13_37_AEV.pdf.

Venice Commission (2007). *Opinion: On video surveillance in public places by public authorities and the protection of human rights,* CDL-AD(2007)014, Study 404/2006. Strasbourg: Council of Europe Retrieved on 04-07-2011 from http://www.venice.coe.int/docs/2007/CDL-AD(2007)014-e.pdf.

White, M. (2008, October 22). 'Call for World Biometric Database', *Sky News.* Retrieved on 15-1-2011 from http://news.sky.com/skynews/Home/UK-News/Global-Biometric-

Database-Interpol-Wants-To-Track-Criminals-Using-Fingerprint-Data/Article/

Witness (2011). 'The Hub: The global platform for human rights media and action'. H*ub Witness.* Retrieved on 23-11-2011 from http://hub.witness.org/

Wood, D.M. and Webster, C.W.R. (2009). 'Living in Surveillance Societies: The normalization of surveillance in Europe and the threat of a bad example'. J*ournal of Contemporary European* Research, Vol.5, nr, 2, pp. 259-273.

Wright, David, and Paul de Hert (2012) (Eds.), *Privacy Impact Assessment,* Dordrecht: Springer.

Zedner, L. (2009). *Security*, London: Routledge.