in:ex

Converging and conflicting ethical values in the internal/external security continuum in Europe

European Commission, 7th Framework Programme

Milestone report 1.5:
Ethical issues relative to technology and surveillance across borders

Milestone report submitted September 2009 (M19) in fulfillment of requirements of the FP7 Project, Converging and Conflicting Ethical Values in the Internal/External Security Continuum in Europe (INEX)

PRIO	International Peace Research Institute, Oslo	PO Box 9229 Grønland NO-0134 Oslo, Norway	T: +47 22 54 77 00 F: +47 22 54 77 01	www.inexproject.eu

Table of contents

SUMMARY **3**

I INTRODUCTION **4**

II KEY FINDINGS **5**

Security technologies and ethics 5

Towards active mistrust 7

A need for alternative modalities 9

III FUTURE WORK **10**

IV REFERENCES **11**

SUMMARY

This milestone report underlines the findings produced by the *WP1 Ethical premises and consequences of security technologies* on the *Human / ethical consequences of pro-activity.* It also presents some of the aims and objective to be pursued by the WP1 in its future research. The report is mainly based on the work prepared in the first deliverable D.1.1. *State-of-Art Review of Scholarly Research on Security Technologies and Their Relation to the Societies Which they serve*, but will also draw on findings from the second deliverable *D.1.2 Catalogue of Security and Border Technologies at Use in Europe*. WP1 acknowledges that a growing attention is brought to the development and deployment of advanced technology in security practices. This is especially evident when looking at border management and transnational surveillance. Nonetheless, little attention is given to the ethical issues the reliance on new security practices give rise to. The introduction of technology into security practices and the ethical debate it give rise to is not a new phenomenon. However, the current security technologies have transformed the practices and meaning of security. Hence, the notion of security has been transformed from; a logic of protection and reassurances to a logic of risk management. This replaces the trust in fellow citizens and third country national with an active mistrust where everyone is viewed as potential perpetrators. Security practices are thus developed within a framework emphasizing proactivity, profiling, and prevention. Anticipation becomes a tool for security professionals who to greater extent claim to know the future, by adapting their behavior towards preventing a future threat from taking place. This may lead to serious effects for movement across borders and certainly contains serious implication for the presumption of innocence, and the certain rights and freedoms of EU citizens. To deal with these issues WP1 call for developing new modalities that will take ethical issues into consideration. The incorporation of ethical principles in the actual development of technologies referred to as privacy by design may become important in this regard. The future research by WP1 will aim to: Analyze the interaction between the private sector, the security professionals, and the community bureaucracies and certain third countries; conduct further research on the security industry; and look more closely at the private and public bodies dealing with surveillance and data protection. WP1 will continue to elaborate and examine alternative modalities addressing ethical considerations. The next step by WP1 will be to prepare and launch a workshop titled: *The imbedded value assumptions and ethical consequences of security technologies* (D.1.4), scheduled for the period M25.

I. INTRODUCTION

Within the general objective of the INEX project which is to contribute to the existing understandings of European security through an analysis of the value-based premises and ethical consequences of the 'internal/external security continuum' in Europe, Working Package 1 (WP1)[1] aims to "clarify the ethically based social and cultural underpinnings of contemporary security technologies in general and their use in the internal and external policing in the European Union, in particular".[2]

This milestone report titled "Ethical issues relative to the technological social control and surveillance across borders" is based on the progress and work so far produced by WP1.[3] The report will illustrate the key findings and presents the relevant issues acknowledged by WP1. The report is mainly based on the deliverable: D.1.1. *State-of-Art Review of Scholarly Research on Security Technologies and Their Relation to the Societies Which they serve*[4], but will also draw on findings from the second deliverable *D.1.2 Catalogue of Security and Border Technologies at Use in Europe*[5]. Both of the deliverables produced by WP1 brings up the notion of technological development in security practices and highlights the lack of attention so far given to the ethical consideration this give rise to.

This report is structured as follows: it will first present the key findings aimed towards highlighting the ethical issues the rapid development and expansion of security technologies gives rise to. It will also present the major aims and focus of future research within WP1, and the next steps to be taken.

[1] The official title of Working package 1 is: *Ethical premises and consequences of security technologies*

[2] Annex I: Description of Work, (2008). INEX Project: Converging and conflicting ethical values in the internal / external security continuum in Europe, prepared 31st January 2008, p. 26

[3] Ibid, p. 26-27

[4] Bigo, Didier, Philippe Bonditti, Julien Jeandesboz and Francesco Ragazzi (2008), *State-of-Art Review of Scholarly Research on Security Technologies and Their Relation to the Societies Which They Serve*, INEX Deliverable D.1.1., Centre d'Etudes sur les Conflits, Paris, November.

[5] Anthony Amicelle, Didier Bigo, Julien Jeandesboz and Francesco Ragazzi (2009). *Catalogue of Security and Border Technologies at Use in Europe Today*. INEX Deliverable: D.1.2. Centre d'Etudes sur les Conflits, Paris, June.

II. KEY FINDINGS

Security practices in the European Union are becoming gradually reliant on technological solutions. These are often subordinated under two general claims: firstly, they sanction a greater efficiency of security agencies and services; secondly, that they are essential to match the alleged growing sophistication of wrong-doers, to improve the capacity of EU security agencies and services to counter them, and hence to make citizens of the EU safer.[6] WP1 have acknowledged that in the ongoing and rapid process of developing and deploying security technologies in the name of security only modest attention is brought to the ethical implication of security practices.[7] The ethical issues that arise shall in this report be further explored based on key findings by WP1.

Security technologies and ethics

Borders and transnational circulation have comprised a key focus for the current development and hence investment in security technologies witnessed in Europe. The currently active EU databases all deal with movement across border (mainly persons). Two major databases, the SIS-II and VIS, are both scheduled to be in function shortly. These will not only deal with matters of movement across borders, but also include the maintenance of personal data. Not yet decided, thus a likely scenario is that SIS-II and VIS will include an EU register for travel documents and identity cards, an EU entry/exit system, and an electronic system of travel authorization (ESTA). This latter will mainly be aimed towards third country nationals traveling into the European Union. Another relatively recent proposal made by the European Commission (EC) on security, is the improvement and eventually deployment of a European border surveillance system, namely EUROSUR.[8] Deployment of such systems shall not be regarded in favor of stopping or reducing mobility which still is an important imperative, but it may create certain ethical question marks.[9]

Bigo, Didier, Philippe Bonditti, Julien Jeandesboz and Francesco Ragazzi (2008), *State-of-Art Review of Scholarly Research on Security Technologies and Their Relation to the Societies Which They Serve*, INEX Deliverable D.1.1., Centre d'Etudes sur les Conflits, Paris, November, p.4

[7] Ibid, p.5

[8] Ibid, p.4

[9] Anthony Amicelle, Didier Bigo, Julien Jeandesboz and Francesco Ragazzi (2009). *Catalogue of Security and Border Technologies at Use in Europe Today*. INEX Deliverable: D.1.2. Centre d'Etudes sur les Conflits, Paris, June, p.49.

The assumption that technologies in respect to security are value neutral seems to underpin the inherent lack of interest on ethical considerations. Technology is seen "as tools to be mobilized in the pursuit of efficiency for the purpose of countering new dangers and risks".[10] In addition policy makers, politicians, security / technology professionals are concerned with the management of a European industrial base for defense and security with the assumption that this might bring reassurances to EU citizens. These concerns tend to oversee the actual implications included in the technological development of security practices in regard to privacy, but also when considering "social justice, the repartition of risks, discrimination and exclusion".[11]

The dominant argument in the discussion on the implication of security technologies for individual freedoms and rights is the notion of everyone's right to security, and that initiatives pursued in the name of security are justified since they will eventually contribute to the protection of EU citizens. In this context some of the technological security practices currently at use fall beyond scrutiny and the scope of democratic investigation. It shall here not be argued that fundamental freedoms and rights by no means are accounted for in the debate about security technologies. However, according to WP1 the underlying assumption on how they are considered contains a serious bias. This bias lies in the basic assumption that reads as follows: "intrusiveness is a requirement for efficiency, and that privacy undermines efficiency".[12] Hence, a stronger reliance and promotion of privacy is viewed as increasing the potential of insecurities. Relying on such assumption would entail that the maintenance of safety for European citizens needs to be pursued on the expense of certain fundamental rights and freedoms.[13]

Necessary to mention is that the discussion surrounding the ethics (and politics) of security technologies is not entirely new. Historically technologies such as biometrics have been used as a means of identification, and since the end of the 19th century technology has played a great role on surveillance and control. However, important to note, embraced by several scholars is that the rapid emergence of security technologies now taking place has transformed "the legitimization, meaning, practices, and implications of security and

[10] Bigo, Didier, Philippe Bonditti, Julien Jeandesboz and Francesco Ragazzi (2008), *State-of-Art Review of Scholarly Research on Security Technologies and Their Relation to the Societies Which They Serve*, INEX Deliverable D.1.1., Centre d'Etudes sur les Conflits, Paris, November, p.5.
[11] Ibid, p.5
[12] Ibid, p.23
[13] Ibid, p.23

surveillance" by supporting a shift from "a logic of protection and reassurance to a logic of risk management".[14]

Towards active mistrust

Risk and how it should be controlled is often viewed as a phenomenon that is socially constructed.[15] The notion of risk in the context of security practices and policies, constituting risk management aiming in particular at modern threats, in particular counterterrorism, hence replaces active trust with active mistrust. The trust and goodwill in fellow citizens and third country nationals are in a sense undermined [16] as individuals to a greater extent are considered as perpetrators. A general dilemma inherent in the practice of risk management can be explained with the idea that "the dissolution of trust multiplies risks", terrorist threats (and other) triggers a "self multiplication of risks by the de-bounding of risk perception and fantasies".[17]

With a shift of security practices towards risk management another important acknowledgement on security technologies becomes evident; namely that the right to security and security in general for EU citizens becomes reliant on anticipation. The reliance on anticipation in the name of security hence provides an environment whereas increased attentions is given to the notion of proactivity, profiling and prevention.[18] All of these constitute a framework highly dependent on technology and that aims to assess a future threat in order to prevent a certain scenario or event from taking place.[19] The stance among security professionals accordingly becomes the one of knowing the future, thus justified by access and knowledge of information and technology that others do not possess such as; secured databases, personal data including details about one's private life or biometric information etc. In addition they must also claim a specific know-how; including profiling techniques and

[14] Bigo, Didier, Philippe Bonditti, Julien Jeandesboz and Francesco Ragazzi (2008), *State-of-Art Review of Scholarly Research on Security Technologies and Their Relation to the Societies Which They Serve*, INEX Deliverable D.1.1., Centre d'Etudes sur les Conflits, Paris, November, p.24; see further Amoore, L., de Goede, M. (2005), Governance, risk and dataveillance in the war on terror, Crime, Law & Social Change;

[15] Douglas M., Wildavsky, A. (1982), Risk and Culture: An Essay on the Selection of Technical and Environmental Dangers, Berkeley: University of California Press.

[16] Bigo, Didier, Philippe Bonditti, Julien Jeandesboz and Francesco Ragazzi (2008), *State-of-Art Review of Scholarly Research on Security Technologies and Their Relation to the Societies Which They Serve*, INEX Deliverable D.1.1., Centre d'Etudes sur les Conflits, Paris, November, p.24

[17] Ibid, p.24

[18] Ibid, p.25; More on the work produced by WP1 on Proactivity see; Milestone 1.2: Human Ethical Consequences of Proactivity, INEX-Project 2009.

[19] Ham, Shane and Robert D. Atkinson (2002), *Using Technology to Detect and Prevent Terrorism*, Progressive Policy Institute, January. P.12.

forms of risk analysis. As a consequence sophisticated technology becomes a major asset since they are considered as a means to know more. In turn this leads to a growth and expansion of the number of actors involved in various security practices, including both the public and private spheres. [20]

This combination of an increased capacity to analyze and scrutinize individuals and the claim to know the future by security professionals is a development that raises serious ethical concerns. By evolving security practices that may expose individuals more visually matter of privacy and also social justice are put at odds. As mentioned above the sense of active mistrust becomes all the more present, but also the very fact of abstract reliability on technology is a matter of concern. Relying on categorization and preemptive models for locating perpetrators may at times prove false and hence threaten the notion of presumption of innocence.[21] An example may be derived from current practices on border surveillance where technology is used in the purpose of sorting out individuals and groups that may be considered as a danger for the safety of EU citizens. In this respect all movements across borders are observed and analyzed with a sense of suspicion.[22] Another dilemma with regard to proactivity, profiling and prevention framework is the understanding that by knowing more, better anticipation of the future is possible. Such an assumption may lead to a *vicious circle* enabling an endless expansion of the information collected. Here issues of privacy and reliability on what type of data that is being collected and who is responsible for collecting and singling out the data becomes matters of concern.[23] WP1 have acknowledged that the ethical issues arising from the transformation of security practices in favor of risk management call for alternative modalities for safeguarding fundamental freedoms and rights.

A need for alternative modalities

Existing modalities for safeguarding rights and freedoms has to a large extent been overshadowed by the notion of a right to security and the technological developments. The limits of existing modalities have been under consideration for quite some time. Scholars have

[20] Ibid, p.25
[21] Ibid, p.25
[22] Anthony Amicelle, Didier Bigo, Julien Jeandesboz and Francesco Ragazzi (2009). *Catalogue of Security and Border Technologies at Use in Europe Today*. INEX Deliverable: D.1.2. Centre d'Etudes sur les Conflits, Paris, June, p.49.
[23] Bigo, Didier, Philippe Bonditti, Julien Jeandesboz and Francesco Ragazzi (2008), *State-of-Art Review of Scholarly Research on Security Technologies and Their Relation to the Societies Which They Serve*, INEX Deliverable D.1.1., Centre d'Etudes sur les Conflits, Paris, November, p.25

advocated for incorporation of basic ethical principles of privacy into security practices introducing the notion of fair information practices. This comprises “informed consent, unitary usage, and non migration of the data’. In Europe this has mainly taken the shape of “informational self-determination” whereas individuals are able to determine what type of data that is being collected about him/her in a given context. Privacy shall in this respect be understood as a “right to opacity” and “the restriction of knowledge and right of access to the personal data for different state agencies”. A crucial question that arises is how to apply fair information practice or informational self determination in a setting where “databases are proliferating, where information is exchanged transnational” but also to a greater extent collected and hence managed through automated processes, involving both the public and private sector, and where the type of information collected contains element beyond daily life including both physical and psychological data? [24]

When multiple and so many organizations and agencies are involves in the data collection, for various purposes and in different settings it seems almost impossible for individuals to be able to make a decision on when to disagree or are, and moreover to reclaim information. In this sense the current transparency and oversight performed by certain authorities, such as data protection agencies, are not regarded as sufficient. In this sense it seems to be a need for alternative modalities or practices that may safeguard the rights and freedoms of EU citizens. One alternative that have been brought up by scholars is the notion of privacy by design. Here privacy considerations are included in the actual development of technological systems. A modality enhancing privacy by design shall not only make individuals aware of what data that is being collected, but is shall also contribute to enhance the inspection of the surviellants themselves, creating a logic of “watch the watchers”. [25] WP1 have concluded that the development and creation of new modalities needs to be given more attentions and will hence constitute an important aim in further research.

[24] Ibid, p.27
[25] Ibid, p.27

III. FUTURE WORK

The future scope of the research will aim to focus on the providers of security technologies in the EU. The interaction between the private sector, the security professionals, and the community bureaucracies and certain third countries will be further researched and analyzed. The workpackage will firstly focus on the different interfaces between the security industry and the community bureaucracies. Examination of certain venues may here become relevant such as the European Security Research Advisory Board (ESRAB) or issue specific arenas like the European Biometric Forum (EBF). Secondly the security providers, namely the industry will be looked at more closely. Here focus will be on both "the designing of technologies for security purposes, on the marketing practices of private companies in the field of security technologies, and on the advocacy strategies with regard the promotion of specific technological products within the European governmental arenas".[26] Efforts will be aimed at including both major companies as for example; EADS, Sagem Security, and Thales, but also smaller firms will be analyzed. The research will also be aimed at looking on whether, and if so how the security industry contributes to the creation of a knowledge and know-how on insecurities, threats and risks. Finally the various bodies both private and public dealing with the protection of data and surveillance practices related to technology will be looked at. [27]

Throughout the future work pursued by the WP1 substantial attentions will at the same time be given to the notion of privacy by design and alternative models for safeguarding EU citizens rights and freedoms. The following questions will be guiding in this process: *Are the existing modalities for the protection of personal data sufficient? Is it possible to place privacy, rather than extensive surveillance, as the basic script of existing and developing technological systems? What are the requirements for an evolving, rather than a fixed, privacy-enhancing system?*[28] Next concrete output from WP1 will be a workshop titled: *The imbedded value assumptions and ethical consequences of security technologies (D.1.4),* scheduled to be held in March 2010 (M25).

[26] Bigo, Didier, Philippe Bonditti, Julien Jeandesboz and Francesco Ragazzi (2008), *State-of-Art Review of Scholarly Research on Security Technologies and Their Relation to the Societies Which They Serve*, INEX Deliverable D.1.1., Centre d'Etudes sur les Conflits, Paris, November, p, 28
[27] Ibid, pp. 27-28
[28] Ibid, p.27.

IV. REFERENCES

Amoore, L., de Goede, M. (2005), Governance, risk and dataveillance in the war on terror, Crime, Law & Social Change, 43. 149-173.

Annex I: Description of Work, (2008). INEX Project: Converging and conflicting ethical values in the internal / external security continuum in Europe, prepared 31st January 2008.

Anthony Amicelle, Didier Bigo, Julien Jeandesboz and Francesco Ragazzi (2009). *Catalogue of Security and Border Technologies at Use in Europe Today*. INEX Deliverable: D.1.2. Centre d'Etudes sur les Conflits, Paris, June.

Bigo, Didier, Philippe Bonditti, Julien Jeandesboz and Francesco Ragazzi (2008), *State-of-Art Review of Scholarly Research on Security Technologies and Their Relation to the Societies Which They Serve*, INEX Deliverable D.1.1., Centre d'Etudes sur les Conflits, Paris, November.

Douglas M., Wildavsky, A. (1982), Risk and Culture: An Essay on the Selection of Technical and Environmental Dangers, Berkeley: University of California Press.

Ham, Shane and Robert D. Atkinson (2002), *Using Technology to Detect and Prevent Terrorism*, Progressive Policy Institute, January.