AFSP Congrès, Strasbourg 2011
ST 21 Politiques de l'immigration : entre justice et démocratie

Elin Palm, Linköping University Post Doctoral Research Fellow
Center for Applied Ethics, Linköping University, Sweden
elin.palm@liu.se

DRAFT VERSION. PLEASE DO NOT QUOTE

Towards an Ethically Defensible Migration Management
- The case of surveillance-based migration control.

1. Introduction

Surveillance technology is increasingly used to control regular migration. Biometric-based e-passports, registers of passenger data and "naked machines" (full body scanners) are examples of systems implemented to verify migrants´ identity and to enhance security. Surveillance regimes are also employed to control the identity and movements of irregular migrants and reduce unauthorized migration.[1] Unmanned Aerial Vehicles (UAVs), infrared CCTV-cameras and sensors, thermal imaging systems, GPS-equipped bracelets and the networking of vast databases are employed for those purposes. Member states making up the external frontiers of the Schengen zone like Ukraine - a source and transit country for irregular migrants - (Uehling, 2004, Düvell, 2008) have strengthened the range and scope of their border protection activities by means of e.g. infrared sensors and binocular thermal imaging systems (Jandl, 2007), typically coordinated by Frontex.[2] More recently, upheavals and on-going conflicts in North Africa have the increased migration flow across the Mediterranean sea and triggered intensified border controls along the international land- and maritime borders of Southern European countries.

Even if EU-member states have agreed on the need to address 'root causes' of irregular migration (European Council in Tampere in 1999), current migration management is foremost

[1] The term "irregular migrants" concerns individuals who enter or stay within a state/region without proper documentation or permits. Unauthorized migrants will be used interchangeably.
[2] The European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union.

characterized by conventional control strategies reinforced by sophisticated surveillance equipment. Data-mining software, biometrics and the various detection technologies in use pose serious ethical problems. Error and misconduct may always occur and technology with the capacity to trace and track individuals can harm fundamental human rights like privacy and dignity. Surveillance may also be used in a discriminating way. Certainly, privacy, dignity, democracy and equality issues have been discussed in relation to surveillance technology (cf. Lyon, 2003, Gandy, 1993, Haggerty and Samatas, 2010) but seldom in relation to irregular migration.

This article discusses some of the ethical implications of surveillance regimes used to control migration and in particular, the effects on irregular migration. A tentative ethical assessment is conducted, investigating: (1) the impact of surveillance device X on fundamental rights and interests Z, (2) whether there is a reasonable aim Y behind the usage of X and (3) whether X is an efficient means to Y.

Even if some form of control of borders and migrants may be necessary, and although surveillance can be motivated, measures should be taken to, as far as possible, minimize negative effects of surveillance technology. Irrespective of whether or not one believes that nation states or the Schengen zone should be in their right to protect their borders and be entitled to do so by means of surveillance technology, questions of reasonable aims and proportional conduct deserve analysis.[3] What reasons are used to motivate surveillance-based migration control? Can those reasons be justified? Arguably, the technology should be maximally effective and minimally intrusive. Ways of reducing the intrusive aspects will be suggested.

Section (2) offers a brief survey of the legal support applying to irregular migrants. In section (3) ethical implications of surveillance regimes employed to control movement across borders is analyzed. Section (4) concludes.

2. Migration – regular and irregular

[3] The legal and ethical justification of pre-border control may for instance be questioned. When migrant vessels are detected by Schengen coast guards during pre-border patrols in the waters of third countries, those are often immediately diverted to the country of origin without allowing the migrants on board to apply for asylum. Diverting asylum-seekers and thereby denying them access to an asylum process may constitute a breach of the *non-refoulement* principle ie. that no person in need of protection should be returned to a country where her life or freedom may be threatened (Hernandez-Carretero, 2009).

Migration is a complex and deeply contested issue that has instigated philosophical debates about: the right of sovereign states to protect their borders (Meilaender, 2001, Miller, 2005), the significance of inequality for migration (Pogge, 1997), the individual's right to decent life chances (Seglow, 2005), just membership (Benhabib, 2004) and the case for open borders (cf. Carens, 1987, 2003, Kukathas, 2005). More empirically oriented discussions often focus relations between globalization and global inequality, movement and control (Held and Kaya, 2006). Commonly discussed are also how power, inequality and movement are related and whether migration reduces or reproduces inequality (World Development Report, 2006). Scarcely recognized but highly relevant are the ethical implications of surveillance technology as a means to control irregular migration.

A focus on irregular migrants is motivated by the relative vulnerability of this group and the risks that they face. A large number of irregular migrants suffer from traumatic experiences (cf. UN Special Rapporteur on Human Rights of Migrants, A/61/324) and undocumented migrants, in particular children and female such, often experience exploitative conditions (Bales, 2000, Koser, 2000, World Development Report, 2006). Surveillance in public and semi-public areas like the workspace is known to influence the behavior of those subjected to surveillance and to induce stress (cf. Margulis, 2003). Most likely, individuals who have been subject to exploitation and undergone traumatic experiences will face extra difficulties to cope with invasive privacy regimes.

Importantly, international law makes up a framework protecting the rights of migrants, regardless of nationality or status. States must protect all migrants' rights both in transit between states and within states. Human rights apply universally and all individuals, irregular migrants included, enjoy certain fundamental rights like the right to privacy and personal data (articles 7-8 of the Charter of Fundamental Rights),[4] respect for human dignity and non-discrimination.[5] Those rights are also emphasized in codes central to migrants´ and border

[4] Article 8 of the ECHR [European Convention of Human Rights] articulates the right to privacy:
"Right to respect for private and family life.
1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".http://www.echr.coe.int/nr/rdonlyres/d5cc24a7-dc13-4318-b457-5c9014916d7a/0/englishanglais.pdf

[5] Article 14 of the ECHR articulates the prohibition on discrimination: "*Prohibition of Discrimination.*

security (Schengen Borders Code and the Handbook and documents concerning border control such as the 2010 EU Action Plan Implementing the Stockholm Program, and the 2008 Updated Schengen Catalogue on External Borders Control, Return and Readmission). Likewise, the prohibition on torture and cruel, inhuman and degrading treatment is found in the Schengen Handbook, and all EU legal documents on fundamental rights and international human rights treaties and conventions.

Importantly, international law acknowledges the special vulnerabilities of refugees and displaced persons as well as obligations on states to assist such people. Children are vulnerable to exploitation and recognized as having rights and obligations that differ from those of adults. Most importantly, the right to seek asylum is a fundamental human right. According to international law, individuals have a right to leave their countries and to return but there are no corresponding rights to enter or remain in another country. Sovereign states may decide on admission, treatment and removal of non-nationals but must respect human rights like the European Convention of Human Rights (ECHR). European minimum standards, drawn from international law and adopted by Council of Europe Parliament Assembly (PACE), hold for irregular migrants in Europe (CommDH/issue paper, 2007).

3. Surveillance-based migration control

Migration control includes a broad range of activities. The following are examples thereof:

(1) pre-border control e.g. Frontex patrolling third country waters in order to detect migrant vessels before illegally entering the Schengen region,

(2) control of legal and illegal entries at authorized border crossings,

(3) control of illegal entries at unauthorized border crossings,

(4) externalized migration control[6] and

(5) surveillance of individuals who are part of an asylum seeking procedure in an EU member state.

The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status."

[6] A novel feature of European migration management in need of better recognition is the increased externalization of migration control to third countries in order to "avert mass influx of people to EU territory" (The Hague Program, Tampere II, Article III-266, 2.g). Origin and transit countries are requested to assist with control activities, process migrants´ claims before they may enter the EU, and to readmit illegal immigrants.[6] Regional Protection Areas (RPA) and Transit Processing Centers are intended as safe havens for migrants and refugees, established by the EU outside the European Union where biometric identification systems may be used to identify and keep track of them. Certainly, those centers are intended to be run by neutral parties such as non-governmental organizations rather than by local authorities. Nevertheless, this may imply an export of surveillance-based migration control to non-democratic societies which raises serious ethical questions.

Here (1), (2), (3) and (5) will be touched upon, leaving unauthorized border crossings and externalized migration control aside although all 5 types deserve ethical analysis.

Before discussing examples of surveillance-based border conduct, a brief definition of the concept surveillance will be given. By "surveillance" is understood: practices that involve information gathering about individuals with the purpose to influence their behavior or control them. Certainly, border control may be of traditional, manual kind e.g. border patrol. However, in most cases border controls are instrumented and automated. Patrolling at sea is most often assisted with high-tech radar systems, camera surveillance systems and UAVs and night vision devices, thermal cameras and sensor alarm systems are used for land border control (Schengen Updated Handbook, p. 37-38).[7] Although surveillance and monitoring often are used as interchangeable terms, here, monitoring refers to information-gathering conducted with a non-specific aim e.g. to deter from illegal border crossing activities in general, whereas surveillance reserved for data collection with a specific purpose.

In below, the following surveillance regimes will be subjected to discussion: (1) biometric identification systems, (2) "Dataveillance" and the networking of databases, (3) detection technologies used to control borders and (4) technology-assisted detention.

3.1 Biometric-based passports

e-passports equipped with radio-frequency IDs containing and transmitting person-specific information are typically considered a means to provide reliable verification of individuals moving across borders and an instrument to combat fraud and identity theft. At present, e-passports are used in more than 60 countries over the world. Increasingly, e-passports also contain digitized biometric data such as fingerprints or iris patterns. The European Union has required of its member states (and non-members like Iceland, Norway, Switzerland and Turkey) to implement biometrics in passports no later than 2012. Biometric features in passports and travel documents will be used to verify the authenticity of the document and the identity of the holder. The information used to identify the passport holder are features unique to the individual such as finger prints, the shape of the ear, and facial features like the distances between eyes, nose, mouth and ears (van der Ploeg, 1999, 2003, 2009). Such information is stable (from 12 years of age) and difficult to manipulate, hence considered a most reliable basis for identification. Passports equipped with micro-chips containing

[7] http://www.enpi-info.eu/files/publications/ethics_of_border_security_report%5B1%5D.pdf

biometric information can be read electronically by machines located in for instance an airport and then compared to the data stored in a central database. Entering the Schengen zone, individuals who do not carry biometric-based passports may have to provide biometric samples at authorized border crossings under the EURODAC system.

The logic behind the implementation of biometrics in passports is that of enhancing security. Although biometrics-based systems are said to provide more reliable identification/verification a number of questions merit further analysis. Any technology generating or relying on person-specific data that is stored, transferred or processed must be secure from outside interference, and certainly general Information Security principles apply to biometric-based passports i.e. the Confidentiality, Integrity and Accuracy of data apply. Furthermore, questions regarding the reliability of the authentication process must be addressed. What are the implications of false positives/negatives? And, related to the dissemination of data: may third parties get access to personal data? Can the chip be read by others than those agencies that legitimately may conduct identity checks? Are there any risks that personal data will be checked against any registers or databases, e.g. run against watch-lists?

Apart from the obvious risks associated with biometrics and facial recognition technology (FR) the specific type of information used in biometric identification systems deserves further attention.

Biometric data is legally protected as personal data (Data directive) and by many, this type of information is considered inherently sensitive. It is said to be a special type of person-specific information in that it concerns unique features that we "cannot" alter and since it serves as a key to other identifying person-related data. Moreover, the case has been made that biometric identification systems affect our identity (van der Ploeg, 1999, 2003, 2009, Altman, 2003). Biometrics serves to verify and authenticate identities has been criticized for the reason that the human body is turned into a machine-readable object (van der Ploeg, 2003, 2009). Irises, voices, fingerprints are transformed into readable "text" and different meanings may be attached to the biometric body and tied to identity, without our awareness.

> *"Biometric data changes irrevocably the relation between body and identity, in that they make the characteristics of the human body 'machine-readable' and subject to further use"* (van der Ploeg, 2003).

Another concern with automated biometric identification system and biometrics based surveillance is that individuals will face greater difficulties to control others´ access to their biometric features than to other types of personal data, and hence, that biometrics may eliminate our chances to anonymity and infringe on privacy (Masiello, 2003).

Although biometrics has gained a reputition as a highly reliable means of identification, it is important to recognize that the reliability of the different biometric identification systems varies. The systems also differ with respect to privacy invasiveness why a careful balancing between security, reliability and privacy should be undertaken. Identification by means of facial recognition is considered the least privacy intrusive alternative since it relies on information available/visible to anyone. However, this is also the least reliable of the biometric methods. From the perspective of security, an individual´s retina is considered one of the most reliable bases for biometric identification. At the same time, retina scanning may reveal additional information, irrelevant to the purpose of safe identification e.g. traces of certain diseases may be detected. This type of information could not be accessed just from looking a person in the eyes. Retina scan and iris scan are procedure-wise, equally invasive. But, since the retina scan implies surplus information i.e. more information than what is necessary for the purpose of identification, iris scanning seems to be the most ethically sound alternative. More to the point, the sensitive nature of biometrics requires careful management of this means of identification. Biometric identification procedures may be experienced as privacy invasive why a respectful attitude among those executing passenger controls by means of biometric identification systems is important. In an attempt to secure ethically defensible conduct among border security staff, it has been suggested that biometric identification/verification technology should not be treated as a water-tight means to verify identity. Fraud should not be assumed on the part of those whose identity is queried. “In all cases there is a trade-off between the false positive and false negative rate and balance must be struck between privacy protection and privacy intrusion”.[8]

3.2 Networking of data bases - Dataveillance

[8]http://www.enpi-info.eu/files/publications/ethics_of_border_security_report%5B1%5D.pdf

EU member states have created a database network of the Schengen Information System (SIS), the EURODAC fingerprint database and the Visa Information System including various types of data aiming at controlling migration flows by identifying and sorting authorized and non-authorized migrants (Broeders, 2007). Networking of vast databases (containing different types of information about visa/asylum applications) makes up a potentially powerful instrument to profile migrants' history of movements. Following the Dublin Convention, the country that a migrant first enters or where she first claims asylum is responsible for her (asylum procedure). Attempting to reach another member state, the asylum-seeker can be retrieved to the first point of entry. Large-scale databases containing biometric data and information about visa/asylum applications have been established to facilitate profiling of migrants' history of movements. Digital traces are intended to track and re-identify migrants and biometric identifiers are collected in order to facilitate return procedures of failed asylum applications by identifying the applicant's true country of origin. That is, the database is intended to prevent irregular secondary movements (asylum-seekers who move in an irregular manner from Schengen member states in which they have already gained protection), multiple asylum claims and simultaneous visa applications (Broeders, 2007).

As with all forms of data management, information security standards apply. Unauthorized access to and inadequate sharing of register data must not occur. Information should only be collected and shared if necessary to obtain a reasonable aim and if a proportionate means to that aim. The desired aim must be clearly specified in advance.

Regarding the efficiency of the system, a general awareness that data-mining occurs may deter some individuals from secondary movements and multiple applications. In Europe however, the largest part of irregular migrants are individuals who have entered a European country in a legal fashion and then having over-stayed their visa (Düvell and Vollmer, 2009). Networking of databases may serve to keep track of multiple applications and may put visa-overstayers´ names on watch-lists, preventing them from re-entering EU but cannot ensure that visitors leave in accordance with their visa terms. Neither can the database help locate visa-overstayers, nor can it assist repatriation. That is, in theory, we may well distinguish between regular migrants e.g. refugees with a right to seek and to enjoy asylum and irregular migrants including people who enter a country by human smugglers or traffickers, without proper documents and individuals who remain after valid documents such as visa or work

permits have expired. In practice however, this distinction is difficult to make. A migrant can enter a country in an irregular fashion but obtain a regular status by applying for asylum. Conversely, a migrant may enter regularly but become irregular by working without a work permit, overstaying a visa or undertaking irregular secondary moves.

A more general critique of networking of data and dataveillance concern the opaqueness of such processes and the underlying criteria. Networking of information related to migrants typically serves to identify and sort individuals who move across borders into categories: desirable/undesirable, safe/risky, admissible/inadmissible (Lyon, 1993, Walsh, 2010). Those categories are seldom openly defined as is the case with links between an individual migrant and profiles. Categories used to sort migrants are said to rely on§ norms regarding threats and security (Inda, 2006). "A skin colour, an accent, an attitude and one is slotted, extracted from the unmarked masses and, if necessary, evacuated" (Bigo, 2007:45). Based on the non-transparent categories, certain migrants are placed in "waiting zones" and assigned identities. By means of surveillance regimes and classification, states do not only control movements but enact the categories and divisions (legal/illegal, alien/citizen) they purport to represent and enforce (Walsh, 2010). To some extent, surveillance-based control affects all migrants. However, whereas tourists and professional workers, in most cases, are subjected to momentary, light-weight border control - "thin surveillance", undocumented workers, irregular- and illegal migrants, are subjected to intensive scrutiny - "thick surveillance" (Torpey, 2007).

Absent access to the criteria underlying dataveillance, evaluations of the efficiency and reliability thereof are rendered impossible. And, without adequate information about the procedure (aims, means, results), the autonomy of those subjected to dataveillance is negatively affected. In cases were migrants are refused entry, necessary and sufficient information should be given for the decision. As in the previous discussion, a match in the system indicating the need for further investigation should be treated with caution. The Schengen Information System (SIS) for instance, register individuals suspected of certain (serious) crimes in watch lists. No automated decisions on individual passengers should be allowed without human assessment (only exceptionally and under strict safeguards) (European Parliament). An understanding for the categories that the systems rely on is also necessary.

In brief, the networking of databases discussed may serve to detect irregular secondary movements and multiple visa applications. The most common "irregular migrant" however, seems to be that an individual enter a European country in a legal fashion and then remains illegally – a problem that the system cannot alleviate. Furthermore, an awareness is necessary that data-mining is (1) opaque, hence preventing assessments, (2) potentially privacy invasive, (3) rely on potentially discriminatory categories (stereotypes) and (4) may produce large numbers of false positives i.e. people who present a positive match with the profile or target but are not in fact suspicious.

3.3 Border security and detection systems

Several detection systems are used to enable automated, continuous border control. Video surveillance (CCTV systems) are frequently used at authorized border crossings like air- and sea ports e.g. to profile individuals, selecting persons for second line checks. In addition to standard CCTVs, infrared CCTV cameras and thermal imaging devices are employed. Those technologies can capture images in the dark and under low-light conditions. Smart cameras are programmed to react automatically to certain stimuli e.g. sudden, quick movements and certain behavior

In public domains, the usage of CCTV and especially the use of Smart CCTV, have been controversial due to the technologies´ privacy intrusive capacity (Armstrong and Norris, 1999, Brey, 2004) and for reasons of social sorting (Lyon, 2003). Some argue that privacy invasions mainly occur where individuals´ reasonable expectations of privacy are frustrated. At authorized entry points and border crossings, the use of CCTV is expected and illegal border entry is reasonably expected to be subject to scrutiny. Following this line of reasoning however, individuals have no reasonable expectations on privacy in public. Irrespective of what should count as reasonable expectations, the extent to which individuals are aware of surveillance is crucial for their chances to self-government. As long as individuals´ know that they are subject to camera surveillance, they can adjust their behavior in accordance with how they wish to be seen by others (Palm, 2007). Covert, automated camera surveillance creates an asymmetry between the agents controlling a certain area and those who are subjected to the surveillance. The latter are not necessarily aware of the cameras. Neither can they consent, nor can they avoid surveillance. And even if they would be aware of camera coverage, they would not necessarily know how the information gathered would be processed and used

(Armstrong and Norris, 1999). Smart CCTV is a form of automated surveillance based on rather stereotypical categories of normal/abnormal behavior (algorithms) - classifications that tend to draw disproportionate attention to minorities.

In the same vein, infrared cameras, thermal imaging devices, unmanned aerial vehicles, radars, seismic and magnetic sensors can operate covertly and may give raise to privacy intrusions without the data subjects´ awareness. Their freedom of movement may for instance be restricted without them being aware the reasons therefore.

If combined into integrated systems, those technologies may continuously follow movements across borders over extended periods of time. Hence, the range and scope of traditional border control is substantially altered. The case has been made that an extended range of migration control by means of early detection systems can serve to protect irregular migrants. Following Frontex, UAVs may prevent casualties at sea. That is, one of three key ambitions of Eurosur - the future European Border Surveillance System - is to: reduce the number of illegal immigrants who die at sea while attempting to enter the EU undetected. Certainly, an increased presence of UAVs along the maritime borders may increase the likelihood that lives can be saved in case of an occurrence. However, viewed in a somewhat broader perspective, order to avoid exhaustive surveillance and the risk of interception, irregular migrants may undertake longer and more dangerous routes, e.g. embarking on extensive open-ocean journeys, crossing vast deserts or dangerous mountain passages or mined territory (Hernández-Carretero, 2009) away from "the rescue infrastructure usually found along established migration routes" (Carling, 2007, Carling and Hernández-Carretero, 2008). Efficient border control must not increase risk. In addition to reactive surveillance along the borders, proactive measures must be undertaken to make unauthorized migration a less attractive option to potential migrants.

3.4 Detention and electronic tagging

Whereas the previously discussed surveillance measures have focused on pre-border and border control, this section concerns surveillance of individuals who are part of an asylum process.

Following the 1999 UNHCR Guidelines on detention of asylum seekers ('UNHCR Guidelines on Detention, asylum seekers should be detained if and only if all alternative

strategies have been exhausted. Nevertheless, the asylum seeking processes vary significantly between member states. Many states use detention to ensure that asylum seekers remain available during the asylum process and for removal in case of reject (Field, 2006). In some cases, it has been used to deter future arrivals. Arbitrary detention, both of asylum seekers and refugees, occurs in several countries. In the UK for example, detention is frequently used for reasons of administrative convenience. Alternatives are applied only when detention space is unavailable (Field, 2006).

The legal and ethical justification as well as the necessity and effectiveness of detention have been questioned (Field, 2006). Effectiveness is said to depend on whether the country is a 'destination' or 'transit' state. Detention and other restrictive measures (see list below) are seldom if ever required in destination states where most asylum seekers wish to remain. Few asylum seekers abscond from their "destination country". Rather, they wish to remain there, and hence also to comply with the asylum procedure. In most cases, continuous reporting is a sufficient means to ensure the availability of asylum seekers throughout the whole asylum process.

Support programs that provide asylum-seekers with access to competent legal advice and guardianship have significantly reduced the number of individuals absconding during the asylum process. It implies a non-intrusive form of control and ensures that asylum seekers understand the consequences of non-compliance. More reasonable and also more efficient alternatives have been suggested such as release on the condition that one (a) register one's place of residence, (b) surrender one´s passport, (c) accept supervision by a designated case worker are more cost-effective than detention, (d) report in a certain office or by designated residence. Asylum seekers´ freedom of movement can also be intentionally restricted by a work permit and by ICT-based surveillance e.g. by electronic 'tagging' and home curfew or satellite tracking (Field, 2006).

UK is the European country that, to the largest extent, has implemented surveillance technology in the field of migration management. Voice recognition technology is used for asylum seekers to report to an office, over the phone, at certain hours. Electronic tagging, including GPS equipped bracelets and satellite tracking, is used to monitor failed asylum seekers likely to abscond (Field, 2006) or who are liable for removal (Rosenzweig et al., 2004). In the same way as criminals on early release, registered asylum seekers are put under

surveillance requiring asylum-seekers to be at home at a certain time (Rosenzweig et al., 2004).

In 2010, the Council of Europe Parliament Assembly (PACE) recommended an investigation of detention of asylum seekers and irregular migrants in Europe in order to safeguard fair procedures (PACE Recommendation 1900, 2010). Even if irregular migrants violate national legislation, they must not be deprived of their rights and their dignity and privacy must be respected. Measures to control the trade in human beings often conflict with human rights. While the UN Convention against Transnational Organized Crime, 2003 aims to prevent human smuggling and trafficking, UN has also emphasized that

> "*Immigrants … even those who are in a country illegally and whose claims are not considered valid by the authorities, should not be treated as criminals*" (The UN Special Rapporteur on the Rights of Non-Citizens, 2003).

These directives may conflict since measures adopted to detect the criminal trading in human beings also may affect individuals (irregular but not illegal) subjected to such activity. The need to stifle the illegal activity of human smuggling and trafficking may justify intensified border controls but measures that are reasonable when combating trade in human beings are not necessarily ethically acceptable means to control the movements of migrants in general.[9] Likewise, the ambition not to treat irregular migrants as criminals may conflict with the practice of biometric tagging of asylum-seekers in the UK.

In most cases such practice fails the necessity test i.e. if not related to high flight risk, electronic bracelets are not justified. Most of them who have received a final rejection of their asylum claim however, pose low risk of absconding. This is most often true about families with young children. In those cases tagging would fail the test of 'necessity' and be an illegitimate restriction of individuals´ freedom of movement (Field, 2006). In addition, asylum seekers who have not committed a crime may perceive of an electronic bracelet as an unjust and socially stigmatizing penalty. Moreover, persons refused entry should be placed in specially designated facilities and not in ordinary correctional facilities, as sometimes happens. People seeking asylum are exercising their rights and not engaging in illegal activity, and should in no way be treated as criminals.

[9] A better differentiation of the main groups of migrants: irregular migrants, refugees and asylum-seekers are needed and security measures so that these groups do not loose their protection needs and entitlements and so that they are not unjustly treated as criminals.

4. Conclusion

Increasingly, sophisticated surveillance technology is used to control movements before and across Schengen-borders and asylum seekers once part of the asylum process. Surveillance device are typically deployed as means to distinguish authorized from non-authorized migrants and to grant or deny access. In order to obtain a satisfactorily EU-level migration management, a unified approach has been called for and Eurosur is under development. Central ambitions behind the Eurosur initiative are (1) to improve the protection of Schengen borders, (2) reduce the number of unauthorized migrants by concerted strategies and (3) to save lives, both by discouraging individuals from undertaking perilous journeys and by detecting irregular migrants in life threatening situations.[10] Surveillance technologies play a key role in the realization of those goals.

Irrespective of whether one would agree that nation states or the Schengen zone should be (1) in their right to protect their borders and (2) entitled to do so by means of surveillance technology, questions of reasonable aims and efficient means to realize those aims still deserve analysis. The aim of this article has been to high-light the need for an ethical assessment of surveillance technologies used to control migration. The technologies´ impact on humanitarian needs and human rights must be carefully investigated. By minimizing intrusive aspects of surveillance technology, irregular migrants´ wellbeing can be protected.

The detection devices discussed enable continuous automated surveillance and extend the range and scope of traditional migration control. In that sense, border protection and migration management may be considered improved and more efficient. When applying surveillance device in order to reduce the number of irregular migrants however, the underlying assumption seems to be that the technology will have a strong deterring effect. Plausibly, exhaustive control measures will discourage some individuals from unauthorized migration. However, individuals who attempt to enter the European Union illegally are often aware of the risks associated with irregular migration and willing to take those risks to escape from poor/insecure living conditions at home. They are also aware of the difficulties to control the long stretched maritime borders despite access to sophisticated surveillance device. In order to substantially reduce the number of irregular migrants, root causes must be addressed, and irregular migration must appear a less attractive option.

[10]http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l14579_en.htm

Current migration management is reactive rather than proactive, relying on traditional – although sophisticated – restriction and control mechanisms. Regarding the aim of reducing casualties, a risk is that with efficient surveillance regimes in place, some people may undertake even more risky journeys to reach enter the European Union (Hernandez-Carretero, 2009). Although an unintended effect, casualties may increase with effective surveillance systems. Hence, the implementation of novel surveillance systems should be preceded by careful risk analyses.

In sum, in order for a surveillance system used to control migration (regular or irregular) to be ethically acceptable, it should be maximally efficient and minimally invasive. It must be based on a reasonable aim as well as make up an efficient means to obtain that aim. Furthermore, it must respect fundamental rights and interests of migrants – irregular as well as regular - and must not impose any additional risks on those subjected to surveillance.

5. References

Alterman, A., (2003) A Piece of Yourself: Ethical Issues in Biometric Identification. *Ethics and Information Technology* 5 (3):139-150.

Armstrong, G. and C. Norris (1999) CCTV and the social structuring of surveillance. *Crime Prevention Studies, volume 10, pp. 157-178*

Bales, K., (2000) *Disposable People: New Slavery in the Global Economy*, University of California Press.

Benhabib, S., (2004) *The Rights of Others – Aliens, Residents and Citizens*. Cambridge, Cambridge University Press.

Bigo, D., (2007) Globalized (in)Security: the Field and the Ban-opticon. http://www.ces.fas.harvard.edu/conferences/muslims/Bigo.pdf

Brey, P., (2004) "Ethical aspects of facial recognition systems in public places", *Journal of Information*, *Communication and Ethics in Society*, Vol. 2 Issue: 2, pp.97 – 109

Broeders, D., (2007) The New Digital Borders of the European Union, *International Sociology*.

Carens, J., (1987) Aliens and Citizens: The Case for Open Borders, *Review of Politics*, 49 (2).

Carens, J., (2003) Who Should Get In? The Ethics of Immigration Admissions. *Ethics and International Affairs*, 17, (1).

Carling, J., (2007) 'Unauthorized Migration from Africa to Spain', *International Migration* 45: 3–37.

Carling, J. & M. Hernández-Carretero, (2008) 'Kamikaze Migrants? Understanding and Tackling High-Risk Migration from Africa', paper presented at the workshop 'Narratives of Migration Management and Cooperation with Countries of Origin and Transit', Sussex Centre for Migration Research, University of Sussex, 18–19 September.

Düvell, F. and B. Vollmer., (2009) Irregular Migration in and from the Neighbourhood of the EU. A comparison of Morocco, Turkey and Ukraine. Overview Transit Migration Report (D10) prepared under the research project CLANDESTINO *Undocumented Migration: Counting the Uncountable. Data and Trends Across Europe*, funded by the 6th Framework Programme for Research and Technological Development under Priority 7 '*Citizens and Governance in a Knowledge-Based Society'* , Research DG, European Commission. http://clandestino.eliamep.gr/wp-content/uploads/2009/11/transit_report_compas_sept091.pdf

Düvell, F., (2008), Ukraine – immigration and transit country for Chechen refugees, in Janda, Alexander; Leitner, Norbert; Vogl ,Mathias (eds) *Chechens in the European Union*. Vienna: Österreichischer Integrationsfonds, Federal Ministry of the Interior, pp. 79-92.

Field, O., (2006) Alternatives to Detention of Asylum Seekers and Refugees, Protection Operations and Legal Advice Section (POLAS) Division of International Protection

Services, 2006/03 United Nations High Commissioner for Refugees, Geneva, Switzerland Available online at **http://www.unhcr.org/protect**.

Gandy, O., (1993) *The Panoptic Sort.* Boulder: Westview.

Haggerty. K. and M. Samatas (eds) (2010) *Surveillance and Democracy,* Routledge, New York.

Held. D., and A. Kaya (eds) (2006) *Global Inequality - Patterns and Explanations*, Polity, Cambridge.

Hernandez-Carretero, M., (2009) Reconciling Border Control with the Human Aspects of Unauthorized Migration, *International Peace Research Institute, Oslo (PRIO).* This Policy Brief was written with support from the European Commission Seventh-Framework project *Global Border Environment (GLOBE).* It also draws on research from the subproject *Migration-Based Threat*, funded by the Research Council of Norway. ISBN: 978-82-7288-307-1 **http://www.prio.no/sptrans/724731520/Reconciling-Border-Control.pdf**

Inda. J.X., (2006) *Targeting Immigrants: Government, Technology and Ethics,* Blackwell Publishing, Oxford, UK.

Jandl, M., (2007) Irregular migration, Human Smuggling, and the Eastern Enlargement of the European Union, *International Centre for Migration Policy Development*, Vienna.

Koser, K., (2000) Asylum policies, trafficking and vulnerability. *International Migration*, 38 (8).

Koser, K., (2005) Irregular migration, state security and human security, *The Policy Analysis and Research Programme of the Global Commission on International Migration*, University College London.

Kukathas, C., (2005) The Case for Open Borders in:. A. I. Cohen and C. H. Wellman (eds), *Contemporary Debates in Applied Ethics*, Oxford Blackwell.

Lyon, D., (ed) (2003) Surveillance as *Social Sorting: Privacy, Risk and Digital Discrimination*, New York, Routledge.

Lyon, D., (2001). *Surveillance Society*. London: Open University Press.

Lyon, D., (2008) Biometrics, Identification and Surveillance. *Bioethics* 22 (9):499-508.

Margulis, S. (2003) Privacy as a Social Issue and Behavioural Concept. In:. Contemporary Perspective on Privacy: Social, Psychological and Political (Issue editor S. Margulis) *Journal of Social Issues*.

Masiello, E., (2003) Privacy Implications of Biometric Surveillance: The Destruction of Anonymity. http://www.betsym.org/Privacy_Biometrics.pdf

Meilaender, P., (2001) *Towards a Theory of Immigration*, Basingstoke, Palgrave.

Miller, D., (2005) "Immigration: The Case For Limits" in:. A. I. Cohen and C. H. Wellman (eds), *Contemporary Debates in Applied Ethics*, Oxford Blackwell.

Palm. E., (2007) *The Ethics of Workspace Surveillance*. Doctoral Thesis, The Royal Institute of Technology, Stockholm.

Peral, L., EU Protection Scheme for Refugees in the Region of Origin: Problems of Conditionality and Coherence. http://www.compas.ox.ac.uk/fileadmin/files/pdfs/Non_WP_pdfs/Reports_and_Other_Publications/Refugees_new%20migrants%20Dec06.pdf

Pogge, T. (1997) "Migration and Poverty" in Veit Bader ed. *Citizenship and Exclusion*, St Martin's, New York and Macmillian, London.

Rosenzweig, P., Kochems, A. and A. Schwartz. (2004) Biometric Technologies: Security, Legal and Policy Implications. Legal memorandum No 12, Heritage Foundation.

Seglow, J., (2005) The Ethics of Immigration, *Political Studies Review*, vol. 3.

Torpey, J., (2007). Through thick and thin: surveillance after 9/11. *Contemporary Sociology* 35(2): 116-119.

Uehling, G., (2004). Irregular and illegal migration through Ukraine. *International Migration*.

Van der Ploeg, I., (1999) Written on the body: biometrics and identity. *Computers and Society* 29:1, 37-44.

Van der Ploeg, I., (2003) Biometrics and the body as information: normative issues of the socio-technical coding of the body. In *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination,* ed. David Lyon.

Van der Ploeg, I., (2009) The illegal body: `Eurodac' and the politics of biometric identification, *Ethics and Information Technology*. Vol. 1. Issue. 4.

Walsh, J.P., (2010) From Border Control to Border Care: The Political and Ethical Potential of Surveillance, *Surveillance and Society*, 8 (2), pp. 113-130.