# Smart Surveillance Technologies in Border Control

Vildana Sulić Kenk, [1] Janez Križaj, [2] Vitomir Štruc, [3] Simon Dobrišek [4]

Cite as: Kenk, V.S., Križaj,, J., Štruc, J. & Dobrišek S., Smart Surveillance Technologies in Border Control, in European Journal of Law and Technology, Vol 4., No. 2., 2013.

## ABSTRACT

The paper addresses the technical and legal aspects of the existing and forthcoming intelligent ('smart') surveillance technologies that are (or are considered to be) employed in the border control application area. Such technologies provide a computerized decision-making support to border control authorities, and are intended to increase the reliability and efficiency of border control measures. However, the question that arises is how effective these technologies are, as well as at what price, economically, socially, and in terms of citizens' rights. The paper provides a brief overview of smart surveillance technologies in border control applications, especially those used for controlling cross-border traffic, discusses possible proportionality issues and privacy risks raised by the increasingly widespread use of such technologies, as well as good/best practises developed in this area. In a broader context, the paper presents the result of the research carried out as part of the SMART (Scalable Measures for Automated Recognition Technologies) project.

## 1. INTRODUCTION

The main purpose of EU border security in general is to safeguard European values and interests, among which are fundamental human rights, rule of law, and the freedom of movement. The main border control measures are border checks, border surveillance and risk analysis. These measures facilitate cross-border traffic, fight against crime and migration management. Border control is traditionally implemented by the use of specially trained law enforcement personnel and special surveillance technologies to monitor and protect borders and border crossing points and to provide safety and comfort for travellers and citizens. The use of 'smart' surveillance technologies considerably increases the reliability and efficiency of the border control measures, as these technologies enable pro-active automatic responses to security incidents and threats as they happen. Border management is a central instrument of border control and as such it usually incorporates large collections of private data. The explosion of global travels has led to the emergence of a new border architecture, which seeks to respond effectively to new demands - facilitating mobility while managing the risk associated with the cross-border travel (e.g., terrorism, organized crime, illegal immigrants). The centrepiece of the architecture are collecting and sharing traveller's data (large databases), using new techniques to verify identity more effectively (biometric information) and using new technology at the borders. The new architecture has to achieve two potentially conflicting goals - facilitating mobility while keeping borders safe - while being cost-efficient, essentially error-free, and it should respect individual's rights and privacy.

As part of the SMART project (SMART, 2011-2014), the identified smart surveillance technologies used in this area have been examined from technical and legal perspectives. The examined technologies were classified into two main categories according to the main border control measures. The first category covers the technologies that are used to facilitate the controlling of cross-border traffic. These technologies include large-scale personal information database systems combined with personal identity verification systems, which largely involve automated biometrics-based authentication methods. Such large-scale integrated systems enable the implementation of Automated Border Checks and are the key technologies for implementing Registered Traveller Programs and Entry/Exit Systems, and these are the main building blocks of the concept of 'smart' borders. The second category comprises the surveillance technologies that are used for the purpose of borderline surveillance and could be categorised as sense-and-detect technologies as well. These technologies include different 'smart' sensing systems and detectors, as well as personal and vehicle detection and tracking systems incorporated into large-scale integrated IT systems that improve the monitoring and reaction capacities of border control authorities with the task of preventing irregular migration and cross-border crime.

# 2. CROSS-BORDER TRAFFIC INFORMATION SYSTEMS

In traditional solution of controlling cross-border travels (manual processing of travel documents and passengers), the border guards have the responsibility to verify that:

- the traveller standing in front of the officer is carrying a valid travel document,
- he/she is the person as claimed in the travel document,
- this person is eligible to enter the country, and lastly,
- this person does not pose a threat to its citizens or institutions.

With the improvement of document forging techniques, the uses of look-alikes and aliases, as well as the time pressure associated to border control processing, it is not surprising that border control authorities are revising the traditional manual approach and considering the deployment of the most advanced surveillance technologies to facilitate a more efficient and reliable controlling of cross-border travels (FRONTEX, 2011). Nowadays, information about passengers travelling between borders is being increasingly exchanged via computerized systems. Large collections of personal data are being incorporated into such systems and advanced data-matching and data-mining algorithms are being used for intelligent analytics and solutions that provide border security decision-making support. For instance, data from Passenger Name Records (PNR) are exchanged automatically between immigration management systems to enable smooth borders process. However, it is not clear what PNR data should reasonably be exchanged, to whom and for what purposes as it could include identification data such as name, date of birth, telephone number; transactional data including the dates of reservations, the travel agent where appropriate, the information displayed on the ticket, the itinerary; financial data including credit card number, expiration date, invoicing address, etc.; flight information including flight number, seat number, etc.; and links to earlier PNR data alongside passport and visa details. (Whitley, 2008)

In the following sub-sections, we briefly describe several existing European and national large-scale border management information systems (VIS, SIS, API, PNR, and others) as well as the systems that are in developing phase (EES and RTP), and briefly analyse them from the perspective of proportionality and privacy impact.

## 2.1 VISA INFORMATION SYSTEM

**Background:** Visa Information System (VIS) was established by the European Council Decision 2004/512/EC in 2004 (Council of the EU, 2004) for the exchange of information regarding short-stay visas in the Schengen area. The purpose, functionalities and responsibilities of VIS are defined in Regulation (EC) No 767/2008 (European Parliament; Council of the EU, 2008), known as VIS Regulation. The main purpose of VIS is to improve administration regarding common visa policy. In this regard, the VIS system should facilitate the visa application procedure and checks at the external border, prevent the visa shopping, and contribute to the fight against fraud, internal terrorism and illegal immigration. Competent authorities can use VIS for examining application and for consulting on decisions to issue, refuse, and extend a visa. Personal data (obtained from the application form), fingerprints and photographs are collected and stored in the system for each and every third-country nationals wishing to enter any EU Member State. All data are stored in the system for a maximum of five years. The system allows two types of search, i.e., verification (one-to-one check) and identification (one-to-many check). Access to VIS data is limited to authorised staff only in order to perform their tasks. The Central VIS, which is located in Strasbourg, is connected via communication infrastructure to every national interface in each Member State.

**Legal framework:** Council Decision 2004/512/EC (Council of the EU, 2004), Regulation (EC) No 767/2008 - VIS Regulation (European Parliament; Council of the EU, 2008) and Council Decision 2008/633/JHA (Council of the EU, 2008).

### 2.1.1 PROPORTIONALITY AND PRIVACY IMPACT ANALYSIS

In the following, we briefly analyse the VIS system features, functionalities and components that may raise proportionality issues, privacy protection concerns and operational risks.

**Centralized database:** There is a risk that once data is collected and stored in the system, it can be connected with other data and used for other purposes than originally intended.

**Links to the application files of persons travelling together:** Linkage between the application files of persons travelling together might lead to revealing some other personal data. In addition, linkage between the application files is not relevant and necessary for the implementation of visa policy (Parkin)

**Data about nationality at birth:** The data about applicant's nationality at birth (beside the current nationality) might have an impact on discrimination, especially if the applicant's nationality has been changed. Moreover, data about nationality at birth is not necessary for the implementation of visa policy. According to the JRC report (Goldstein, Angeletti, Holzbach, Konrad, & Snijder, 2008), information on approximately 20 million visa applicants will be stored annually in the system and with a five year retention period; this could lead to no less than 70 million fingerprints data stored at a time. Therefore, the VIS will be the largest biometric database in the world. With the use of such a huge collection, some technical issues, for example performance or error rates, arise.

**Potential function creep:** VIS database supports common visa policy; however, one of its aims is also to help to fight against terrorism although it has no direct connection with the EU's counter-terrorism strategy. In contrast to SIS, which pursues law enforcement purposes, VIS should not be seen as a 'multifunctional tool' and it should be used only for the implementation of EU visa policy. According to the Council Decision 2008/633/JHA (Council of the EU, 2008), access to VIS data is limited (only on a case-by-case basis) for the specific purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences as referred to in Council Framework Decision 2002/584/JHA on the European arrest warrant and the surrender procedures between Member States (Council of the EU, 2002). Tzanou (Tzanou, 2010) argues that access is allowed on the basis that 'it is essential in the fight against terrorism and other serious crime to have the fullest and most up-to-date information in their respective fields'. This kind of decision has effects on privacy and fundamental rights (e.g., third-country nationals are regarded as potential threats to security, which belongs to the discrimination issue - Article 21 EUCFR (European Parliament; Council of the EU, 2000)).

Although VIS Decision regulates the access to VIS data by law enforcement authorities by a number of data protection safeguards, it is still problematic from the right to personal data protection point of view. More precisely, there is a specific data protection principle that suffers particularly by the Decision granting access to VIS data: the purpose limitation principle. The 'purpose limitation principle' - that is, according to the Data Protection Directive (European Parliament; Council of the EU, 1995), the principle that establishes that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes - is a fundamental principle of the EU data protection regime (Tzanou, 2010). For this reason, scope and purpose of the database along with the access to the database should be strictly defined; otherwise there is a possibility of 'function' or 'competence creep' (i.e., when collected data is used for completely different purposes than stated). In order to obtain a visa, traveller agrees that his/her data is collected, consulted and transmitted only for that purpose. Granting access to that data to law enforcement in order to combat terrorism and serious crime constitutes a disproportionate intrusion in the privacy. Furthermore, the fact that law enforcement authorities are granted access to such a vast amount of data entails the risk of profiling individuals on the basis of the information held on them into VIS. This might lead to an infringement of other fundamental rights beyond the right to privacy of the individuals concerned (Tzanou, 2010).

## 2.2 SCHENGEN INFORMATION SYSTEM (SIS I AND SIS II)

**Background** : A collection of data relating to immigration, policing and criminal law is known as Schengen Information System (SIS). It consists of personal data such as, data related to persons wanted for arrest or under surveillance, missing persons, persons to be refused to entry or stay in the Schengen area, data about stolen vehicles or vehicles under surveillance or specific check, data about stolen documents, etc. In addition, the upgraded SIS (known as SIS II) will include biometric information as well, such as photos, fingerprints and, if necessary, also DNA profiles. The reason for the inclusion of biometrics lies in the growing difficulties to search the identity in the system using only the name. Data stored in the SIS database serve as alerts and are needed for the purpose of law enforcement and immigration control in each Member State. Each Member state supplies the system with the data that is needed for issuing an alert and therefore there are some discrepancies regarding the retention period. In general, data is stored for three years; however, this period can be

shorter or longer, depending on each Member State and its national law. Central system, C-SIS, is located in Strasbourg and is connected via SIRENE network to national systems (N-SIS) in each and every Member States.

**Legal framework:** The Schengen *Acquis* - CISA (Council of the EU, 2000), Title 4 - The Schengen Information System (Convention, 1990) and Regulation (EC) No 1987/2006 Schengen Information System - SIS II (European Parliament; Council of the EU, 2006).

#### 2.2.1 PROPORTIONALITY AND PRIVACY IMPACT ANALYSIS

**False positives:** When such large information systems (as e.g., SIS) are used for the checking and comparing the data, they might produce so-called false positives (people who present a positive match with the profile or target but are not in fact suspicious), therefore, the outcome of such searches should not be taken as granted and border guards should be aware of this limitation.

**Different reasons for entering alerts:** Member states have adopted different interpretations of the notion of what constitutes a risk to security and public policy and therefore, this is the main reason for data quality. Two new principles for entering alerts in SIS II are introduced in the Regulation (EC) No 1987/2006 (European Parliament; Council of the EU, 2006), namely individual assessment requirement (i.e., for each individual case member state should consider whether the national criteria and criteria of the Regulation are met) and proportionality clause (i.e., member state should determine if the particular case is adequate, relevant and important enough to warrant entry of the alert in SIS II). Nevertheless, it is expected that discrepancies between the national reporting practices will remain (Parkin, 2011).

**Interlinking of alerts:** Although interlinking of alerts might be a great tool for policing purposes, it also affects individuals and their rights, especially third country nationals. Interlinking allows 'intelligence' logic to creep into the use of the system. Further, allowing associations between the alerts that originate from different motives might have effects on the purpose principle as well as on stigmatisation of certain categories of individuals, i.e. third country nationals seeking entry and residence in the EU.

**Purpose limitation principle:** Since SIS database contains both law enforcement information (e.g., persons wanted for arrest) and border control and immigration information (e.g., banned third country nationals), it contravenes the principle in data protection law (Article 8 EUCFR: 'data must be processed fairly for specified purposes'). This leads to the case where individual, who is registered in SIS for immigration reasons, might be at greater risk of becoming the targets of criminal law enforcement measures or secret surveillance, which may further lead to infringement of fundamental rights (discrimination).

### 2.3 PASSENGER NAME RECORD AND ADVANCED PASSENGER INFORMATION

**Background:** Passenger Name Record (PNR) is the name of the record created when one makes a travel reservation. It contains different information about the person or about the group of people travelling together and about services provided by airlines, tour operators, hotels, etc., e.g., personal information, special meal requests, medical requests. The PNR system was developed by the airlines taking into account their own commercial needs; nevertheless, due to security reasons (e.g., fight against terrorism) some countries require airlines to provide them with some PNR data prior the passenger's entry into the country (e.g., USA, Canada, Australia, and New Zealand). Note that PNR is not an instrument for a border control. Advanced Passenger Information (API) system is also carried out by airlines but in contrary to PNR, it is on behalf of governments. Limited data (i.e., passport information and basic flight information) can be electronically interchanged between the computer system of the airline or origin state and the computer system of the destination state using API system. Again, for security reasons most countries require airlines to transmit passenger's API by the end of check-in.

**Legal Framework:** E.g., EU - U.S. PNR agreement (Council of the EU, 2011), EU - Australia PNR Agreement (Council of the EU, 2011), Council Directive 2004/82/EC -API (Council of the EU, 2004).

#### 2.3.1 PROPORTIONALITY AND PRIVACY IMPACT ANALYSIS

The amount of personal data held in PNR is worrying, especially because it contains data of a sensitive nature. Although there are some data collected for PNR that are inappropriate, the one that stands out is 'general remarks including Other Service Related Information, Special Services Information and Special Service Requests'. The categories included in this field can reveal data related to religious beliefs or related to health and are therefore even more problematic since they can lead to the discrimination.

**Sensitive data in PNR** (i.e., personal data that can reveal religious beliefs, racial or ethnic origin, health, etc.): PNR contains also data of a sensitive nature that might reveal religious beliefs or health issue and might further lead to the discrimination (e.g., meal choice can reveal religion). According to EU-US PNR Agreement sensitive data should be filtered and masked out by the US Department of Homeland Security and deleted in 30 days; however, sensitive data may be retained for the purpose of a specific investigation, prosecution or enforcement action as long as specified in the U.S. law. Contrary, according to the Agreement between EU and Australia, any processing of sensitive data is prohibited and if by any chance transferred PNR data contain sensitive data, the Australian Customs and Border Protection Service should delete it immediately.

**Retention period in PNR:** The main concerns raised here are, why data is only anonymized and not deleted instead and why anonymized data is still needed. Further, what happens to the data that have already been transferred onwards to third countries? Article 8, Paragraph 6 of the EU - U.S. PNR agreement (Council of the EU, 2011), for instance, states that the necessity of a 10-year dormant period of retention will be considered. It is unclear why such long period is needed.

**Wrongful profiling:** Large-scale information system, like PNR and API, have bigger possibility of error and therefore the outcome of such search can produce wrong profiling of individuals and this could further lead to the unfair treatment of innocent people being treated as if they were criminals and this may result in potential infringement of fundamental rights.

**PNR locator number in API:** Among all types of data in API collection there is also one that allows authorities to gain even more information about the individual and this data is PNR locator number. The exposed PNR locator number allows authorities to access PNR database and therefore, more data are available to authorities. It is also not clear, why is the retention period almost longer than a life-time of a particular person.

## 2.4 EURODAC

**Background:** EURODAC is an information system based on fingerprint database, which is used for identifying the Member State responsible (Dublin Convention) for particular asylum application. EURODAC helps to facilitate the application of Dublin Convention. Fingerprints are collected and then stored in the database from each and every asylum-seeker or foreign national found illegally within the EU territory. In addition to fingerprints, the data include also applicant's gender, place and date of the application, reference number and EU country of origin. All data are usually kept for ten years, unless applicant obtains citizenship - in this case all applicants' data are erased immediately. EURODAC consists of a central unit in Luxembourg and national access points, which are connected via secure network to the central part.

**Legal framework:** Regulation (EC) 2725/2000 (Council of the EU, 2000)and Regulation (EC) No 343/2003 - Dublin Convention (Council of the EU, 2003).

### 2.4.1 PROPORTIONALITY AND PRIVACY IMPACT ANALYSIS

**Possible function creep** (collected data might be used for some other purposes): The proposal for a Council Decision on access to EURODAC for law enforcement purposes. In May 2012, a new proposal for an Amended EURODAC regulation was presented. It merges amendments for the better functioning of EURODAC and access to the system by law enforcement. The proposal that EURODAC should also be made accessible for law enforcement authorities and Europol (as VIS) in order to fight terrorism was justified by the Commission on the basis that fingerprint data is especially useful information for law enforcement purposes, as it constitutes an important element in establishing the exact identity of a person. In mid-December 2012 Civil Liberties Committee of the European Parliament voted for allowing the access to EURODAC database to law enforcement bodies in order to investigate terrorism and serious crime; however, due to the change of original

purpose of EURODAC, they demand strict data protection safeguards to avoid interference with the right to privacy and family life of asylum-seeker or refugee. These safeguards include for example a notice to applicants that their data might be used also for law enforcement purposes or that querying the database should be proportionate with the public security concern. In such case, a national level request is needed and if approved (i.e., conditions for requesting an access are met) the designated authority could then access database via national access point. A record of each search conducted by law enforcement authority should be kept (European Parliament, 2012). Despite all safeguards, there are still some negative impacts on individuals that remain. Access to the database by law enforcement may further lead to the stigmatisation or discrimination of vulnerable group of people - asylum seekers or refugees would face greater likelihood of being subject to investigation than other, whose fingerprints are not collected despite the fact that they are not suspected or charged with any crime. This is especially important due to the possibility of false match (error in matching fingerprints) and consequently wrongful implication of asylum-seekers in criminal investigations.

**Fingerprint errors:** There have been concerns whether the technical reliability of the biometric identification within EURODAC is of an appropriate standard. There are several types of errors that need to be considered when evaluating the performance of biometric identification systems, namely the so-called 'Failure to Capture Error' (FCE), 'Failure to Enrol Error' (FEE), 'False Match Error' (FME), and 'False Non-match Error' (FNME). At fingerprint systems vendor tests, only FME and FNME are usually estimated, and, for fingerprint matching systems, FNME at FME = 0.1 % is estimated between 0.1 and 1%, although official figures vary and are subject to different interpretations (BEST, 2010). This means that in average 1 to 10 genuine fingerprints out of 1000 are wrongly rejected as non-match, if 1 impostor fingerprint out of 1000 is wrongly accepted as match.

## 2.5 NATIONAL ENTRY/EXIT SYSTEM AND REGISTERED TRAVELLERS PROGRAMS - EU SMART BORDERS INITIATIVE

**Background:** According to the report on the EU's New Border Surveillance Initiatives (Hayes & Vermeulen, 2012) some 300 million people - just under half of them non-EU citizens - are estimated to enter and leave the EU every year. To enhance border checks on third-country nationals entering the Schengen area, smart border initiative focuses on two issues, i.e., simplifying and facilitating border crossings for those travellers that are pre-vetted and deemed not to pose a security risk to the EU (Registered Travellers Program - RTP) and identifying/preventing 'overstayers' (Entry/Exit System - EES). The initiative for EU RTP foresees the system that would allow certain third-country nationals after an extensive pre-screening process to use automated border control and therefore, it would have effect on the facilitation of border checks. Some EU countries (Germany, Spain, France, Netherlands, Portugal, Finland and United Kingdom) have already implemented a sort of national RTP for EU citizens (automated border checks); however, these systems are not intended for the third-country nationals since current EU rules require border guards to interview a traveller and manually stamp his/her travel document and these are the processes which cannot be automated (European Commission, 2011). The establishment of the EU EES would be the answer to the current problem of the lack of registration of 'overstayers' which constitute the largest group of irregular migrants in the EU (Polish EU Presidency, 2011). EES would record entries and exits of each and every third-country nationals and would also calculate the authorised stay and in the case of overstay, it would raise an alert. There are some EU countries that have implemented a sort of national EES (e.g., Finland, Estonia, Latvia, Lithuania, Poland, Slovakia, Hungary, Romania, Bulgaria, Cyprus, and Portugal). Unfortunately, entry/exit records can be matched only if a traveller lawfully exits the same country, which he/she entered.

**Legal framework:** Up to now there are yet no legislative proposals on the EU's smart borders initiative.

### 2.5.1 PROPORTIONALITY AND PRIVACY IMPACT ANALYSIS

**Possible infringement of fundamental rights and rights to privacy:** Enrolment in EU RTP is voluntary, i.e., a traveller accepts pre-screening of his/her personal and biometric data (face scans and fingerprints) in exchange to faster border check; however, this might result to more extensive and excessive collection of personal data only of third-country nationals travelling to and from EU. Refusal of giving personal and biometric information or failing to register can further lead to the fact that traveller is suspicious and is viewed as a risk.

**Overstays:** The 'overstayer' should have the right to explain the circumstances of an overstay; however, EES will not be able to catch those, who illegally overstay in the EU and therefore, the necessity of implication of EES is questionable.

## 2.6 AUTOMATED PERSONAL IDENTIFICATION SYSTEMS

**Background :** Automated biometric identification systems are used to provide effective automated personal identification process for controlling cross-border travels. Such systems are most often used in combination with the cross-border traffic information systems that are described in the previous section. A biometric automated system usually consists of a sensor that captures individual's characteristics, a storage media for templates (central database or smart card), and a system that verifies the obtained data with the stored data (e.g., fingerprints, images of the face, hand geometry, image of iris). Individual's biometric data can be stored in a central database or on a smart card. In both cases, the authentication is done by comparing user's biometric data to the data stored in a database or to the data stored in the smart card.

### 2.6.1 PROPORTIONALITY AND PRIVACY IMPACT ANALYSIS

**Central database v Smart card (storage media for templates):** There is always a concern over the loss of privacy and potential misuse of data stored in a central repository. Using biometric data (e.g., fingerprints, iris patterns) each and every individual can be uniquely identified and, therefore, the same data can be used also to track individuals, linking many separate databases (the person's whereabouts or purchased items, etc.). Furthermore, there is a possibility that this central database can be used for unintended purposes (e.g., using latent fingerprints for searching for information about a person). Additionally, biometric data may reveal certain rare health problems, which raises another concern regarding possible discriminatory uses of such databases. Although it seems that use of smart card is the most suitable for biometric personal identification systems, there are some deficiencies also in that case. For example, forgers can claim that their card is broken and therefore, they can avoid biometric verification. Due to the fact that a smart card might be damaged in legitimate way, such a situation could be solved by an additional non-biometric authentication or by resorting to a central database (Biometrics Research Group, 2011).

**Errors:** Whenever biometric information is used in the system for matching the individual's identity, there is a trade-off between the false positive and false negative rates. Border guards should be aware of such limitation, although in the context of border security, letting people through who should not be is likely to be considered less acceptable than innocent people having their identity questioned (Frontex, 2010).

## 2.7 AUTOMATED VEHICLE IDENTIFICATION SYSTEM

**Background:** Automated Vehicle Identification System (AVI) is a system for monitoring and controlling vehicle cross-border traffic. Such systems are mainly based on Automated Number Plate Readers (ANPR). These systems are normally used to store the images captured by the cameras as well as the text from the license plate. Some ANPR systems also store a photograph of the driver. The obtained vehicle licence number is then automatically matched with the licence numbers that are stored in various kinds of databases, like the SIS databases of stolen vehicles and similar.

### 2.7.1 PROPORTIONALITY AND PRIVACY IMPACT ANALYSIS

ANPR system is not intrusive by its nature if it is used for a legitimate border control purpose (i.e., controlling vehicles cross-border traffic), nevertheless, the system might be misused for tracking individual's whereabouts. As mentioned, data that is usually collected in a typical ANPR system are, besides vehicle licence numbers, vehicle photographs and photographs of drivers. The latter do not seem to be necessary unless the ANPR application aim is not only automatic vehicle identification but personal identification of drivers as well.

# 3. TECHNOLOGIES FOR BORDER SURVEILLANCE

Border surveillance is, by its nature, mainly an overt surveillance, i.e., everybody is aware that border areas (borderlines or border crossings) are usually under heavy surveillance. Technologies for border surveillance that are based on different kinds of automatic personal and vehicle detection and scanner systems (CCTV, UGV, UAV, UGS, X-Ray devices, Knife

Arches, etc.) rarely involve personal data. The use of surveillance technology at legal border entry points is expected and is therefore only moderately intrusive because it is understood that entry points are highly public places. However, from the operational viewpoint, surveillance of travellers should be proportionate to the legitimate border control aims and planned according to a proper risk analysis. The proportionality of border surveillance should also be analysed from the perspective of its impact on all privacy rights like bodily privacy and human dignity.

## 3.1 DIFFERENT SENSING AND INTEGRATED SYSTEMS

**Background:** Border surveillance is usually based on human involvement. Due to the relatively high cost of the increasing number of personnel as well as the diminishing accuracy through human-only surveillance, the involvement of high-tech devices in border patrol is needed (Sun, et al., 2011). This involves Unmanned Aerial Vehicles (UAVs, also known as drones - small unmanned aircrafts) for aerial surveillance (e.g., automatically detecting illegal crossings), or Fibre Optic Sensors (FOSs), which are buried in the ground to measure pressure waves in the earth caused by intruders or similarly Unattended Ground Sensors (UGSs), which come in three main forms, i.e., seismic, magnetic and infrared, and can detect ground movement, which indicates that someone or something is crossing the border. Additionally, wide area surveillance systems comprising ground radar with thermal infrared and visible wavelength sensors are integrated with intelligent video assessment (IVA) systems. An example of such an integrated surveillance system is, for example, U.S. border - SBInet. This system comprises UGS, UAVs and RVSS (Remote Video Surveillance System - colour and thermal cameras with pan-tilt ability, mounted usually on high poles) or MSS (same as RVSS but has additional mobile component)

Due to a large number of illegal immigration, noticed mainly at the southern parts of Europe (e.g., 13,424 in 2008 at Spanish coastline), many surveillance technologies such as radars and sensors (SIVE - Spanish Integrated System of External Vigilance) and satellite tracking system (SEAHORSE - a network of eight-member countries including Spain, Portugal, Morocco, Mauritania, Cape Verde, Senegal, Guinea-Bissau and Gambia) have been already deployed. Furthermore, there is a proposal to establish a mechanism called European Border Surveillance System (EUROSUR), which would use the state-of-the-art technologies, such as satellites, unmanned aerial vehicles and radar - all integrated into one network and help Member States' authorities to carry out border surveillance activities. The effect of sharing operational information and cooperation between the Member States and with the FRONTEX agency, should reduce the loss of lives at the sea and the number of irregular immigrants entering the EU undetected, while increasing internal security by preventing cross-border crimes (e.g., trafficking in human beings or smuggling of drugs) (European Commision, 2011).

### 3.1.1 PROPORTIONALITY AND PRIVACY IMPACT ANALYSIS

**Possible function creep** : Drones, satellites and high-resolution cameras can be used for example to detect migrant vessels at sea, but cannot do anything to help or prevent in such situations - they can be categorized as sense-and-detect technology. There is a possibility also to misuse such technology for spying also on irrelevant events. There are some concerns that the data UAVs acquire can be 'correlated with information from mobile devices and smart meters and may become an important component of the growing digital record of nearly everything we do' (Villasenor, 2012), especially if they would be used for surveilling other areas, such as routes and speed of every vehicle on the streets or observing the movements of individual pedestrians. At night, they might capture the precise moments when the lights in living rooms and bedrooms are turned on and off, etc. There are also concerns regarding 'drone hacking', which means that the drone operations might be remotely intercepted and compromised to pose a threat to the security of lawful drone operations.

**Application aims:** The following rules for using UAVs should be defined: purpose of UAVs use; who will authorize the use and under which circumstances; specific kinds of information that UAVs should collect; image retention period; data privacy protection and other safeguards. Although there is a general rule about processing personal data only on an exceptional base, the data exchange with other countries might jeopardise individual's rights, particularly in the case of detecting migrants (e.g., the risk that data can be used to identify people who are at risk of being tortured or are subject to some other fundamental rights violations) (Gurzu, 2012). Similarly, there is also a concern regarding EUROSUR and its possible interference with people's right to seek asylum. The reason lies in the fact that

EUROSUR is more focused on preventing people reaching the EU territory than on saving life (migrants would be returned to the country they sailed off).

## 3.2 ADVANCED IMAGING TECHNOLOGIES

**Background:** In the last decade, many advanced imaging algorithms have been developed. Such algorithms can be applied to CCTV networks and therefore can lower monitoring video footage manually and further expanding their coverage. Such computerised systems (e.g., automated number plate recognition -ANPR, face recognition, gait recognition and complex activity recognition) can scan hundreds of video streams, where non-critical events can be saved in the database and used later if needed or in the case of critical event, the system can direct the operators attention to this particular event (Wright, et al., 2010).After the terrorist's attempt to blow up an airplane flying from Amsterdam to Detroit with plastic explosives he had hidden in his underwear, some changes were adopted in the airport security. Due to the ability of scanner technology to detect both metallic and non-metallic items carried on a person, a new EU legislation on security scanners was adopted in 2011. This legislation allows airports and Member States that wish to use security scanners for the screening of passengers, to do so under strict operational and technical conditions (e.g., security scanners should not store, retain, copy, print or retrieve images; any unauthorised access and use of the image is prohibited and should be prevented; the human reviewer analysing the image should be in a separate location and the image should not be linked to the screened person, etc.). These new rules ensure that where this new technology is used it will be covered by EU wide standards on detection capability as well as strict safeguards to protect health and fundamental rights (European Commission, 2011).Using novel sensors, there are also other types of data that can be monitored, e.g., infrared and microwave sensing, infrastructure sensing (e.g., smart power meters), chemical sniffing, rapid DNA analysis and neuro-imaging (brain wave scanning); however, these kind of systems are beyond the scope of this paper and therefore we will not refer to them.

### 3.2.1 PROPORTIONALITY AND PRIVACY IMPACT ANALYSIS

Using surveillance technology (e.g., CCTV, UAVs, IR) at legal border entry points is expected and is therefore only moderately intrusive because it is understood that entry points are highly public places (Frontex, 2010). Nevertheless, surveillance of travellers should be proportionate and planned according to the risk analysis.

**Effectiveness concerns:** With regards to body scanners, there are some issues that arise around the question should body scanners be used at the airports (and later in all other transportation systems). These issues concern mainly the ineffectiveness of scanners (reports on high error rate, possibilities that prohibited items will not be detected), privacy issues, and costs (the cost of one scanner is 100,000 to 150,000 €). There are some reports, which point out that the error rate of body scanners is too high. For example, Germany has abandoned plans to use scanners at its airports due to the high error rate during the testing phase (i.e., up to 40 % error rate) (Watson, 2011; Herald Sun, 2011). Italy reported that during their testing, it took much longer to check the person by a scanner than with a manual inspection and that privacy measures reduced the scanners' effectiveness (Euronews, 2010). Nevertheless, body scanning equipment will be rolled out to all Australian international airports, despite lingering concerns about their effectiveness (Herald Sun, 2012; Parliament of Australia, 2012). Furthermore, the Department of Homeland Security in the US also continues to roll out hundreds more of the scanning machines into airports across the country, claiming that the machine have passed rigorous safety and efficiency tests (Infowars, 2011). There are also some airports in the EU that use scanners, such as UK airports - Gatwick, Heathrow and Manchester (GOV.UK, 2012) and Amsterdam Airport Schiphol (Schiphol, 2012). It is reported that Schiphol is the only airport in the world with Security Scans provided with a screening technology that safeguards personal privacy. A computer analyses images instead of a human operator by means of harmless millimetre wave technology (Schiphol, 2012).

# 4. CONCLUSIONS

At a first glance, most of the investigated technologies employed for border control in Europe seem to be proportional to their application aims. This holds especially for the large-scale information systems used for controlling cross-border traffic, like VIS, SIS, and EURODAC. Operational statistics of security incidents that have been detected and processed in recent years by these systems provide some evidence that they fulfil their main application goals. These systems are also under relatively strict supervision and subjected to

unannounced and announced inspections of the European Data Protection Supervisor authority. As mentioned, for instance, the EDPS inspectors found in 2012 that the overall level of data protection and security of the EURODAC Central Unit is high, and further, that the provisions of the EURODAC Regulation with regard to the data processing are being respected (types of data recorded, data retention periods, specific requirements for advance deletion and blocking of data, etc.). However, the main concern raised by the use of such large-scale information systems is that they are based on centralized databases and once the information has been collected and stored in such databases it can be very easily used for other purposes than originally intended. Classic examples of such a function creep are large-scale passenger information systems like PNR and API that had not been originally created for law enforcement purposes and border control. Such systems and the data types accessed and processed for law enforcement purposes should be subject to a very strict supervision of independent data and privacy protection authorities. Additional proper impact assessments and proportionality analyses are required for these systems to enable further improvement with respect to their use in border control.

The most critical step carried out as part of the border check procedures in general is identity verification. Biometric matching of, for instance, fingerprints, iris, and face images is being increasingly used as a high-tech identity integrity management tool in border control as well. It is well known that biometric technologies in general raise many ethical, sociological, cultural, operational and legal issues with respect to data protection and bodily privacy. In particular, capturing of fingerprints is culturally associated with the exercise of power in relation to criminal law, and this may have negative impact on the dignity of the individuals being involved in such identity verification procedures. A promising option of a privacy-enhanced technology in association with the large-scale border-control personal information systems is the concept of an Intelligent Software Agent that is capable of acting autonomously in order to accomplish a task on behalf of its user in a complex network environment, like personal data ecosystems. Such systems would provide a personal control over personal data. The right step in this direction is an attempt to build the EU Biometric Matching System, under condition that it is implemented as a proper personal data ecosystem.

New advanced surveillance technologies are constantly being developed and deployed for operational use or demonstration purposes in border control, especially for border surveillance purposes. UGVs, UAVs, UGS, Aerostat Surveillance System, motorized CCTV cameras with advanced video and audio analytics surveillance systems that are used for border control rarely involve private data and are considered to be moderately intrusive because it is understood that borderlines are normally under heavy surveillance and border crossing points are highly public places. Nevertheless, such new systems are often not properly assessed from the proportionality perspective as well as from the perspective of data and privacy protection. The main question that should be further addressed by the SMART project and policy-makers in general in this field is how to establish a sound supervision and monitoring system within which it would be clearly stated who, when and how should carried such analyses and assessments. In fact, this task could be assigned to technology developers, law-enforcement and other government agencies, courts, information commissioners, parliamentary committees, independent non-government organisations, as well as to the research projects like to this one. Further, such analyses and assessment could be carried out during the development of the surveillance technology at stake, after the demonstration events, or even after its deployment. And last but not least, such an analysis could be carried out qualitatively and subjectively by consulting all the involved stakeholders and summarizing their professional positions, or quantitatively by using the methodology based on questionnaires and statistical analysis of the answers provided by the involved experts and stakeholders. For example, the U.S. SBInet (integrated electronic border surveillance system) was terminated in 2011 since it was proved to be too costly and problem-plagued. This example shows how important is to make a proper proportionality analysis prior to the actual deployment of large-scale and expensive advanced surveillance technologies for border control, and how easy is to make mistakes in such a decision-making process.

## BIBLIOGRAPHY

BEST. (2010). *Biometrics in Europe: Inventory on Biometric Data and Privacy Legislation.* Retrieved from Biometrics European Stakeholders Network: http://www.best-nw.eu/_fileupload/Deliverables/BEST_deliverable_7%202%20final.pdf

Biometrics Research Group. (2011, December 16). *Biometric Privacy.* Retrieved from Sabanci University Biometrics Research Group: http://biometrics.sabanciuniv.edu/privacy.html

Convention. (1990). *Title IV - The Schengen Information System - Establishment of the Schengen Information System.* Retrieved from http://www.hri.org/docs/Schengen90/body4.html

Council of the EU. (2000). Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention. *Official Journal of the European Union, L*(316), 1-10. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000R2725:EN:PDF

Council of the EU. (2000). The Schengen acquis - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks, *Official Journal of the European Communities, L*(176), 1-473. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:239:0001:0473:EN:PDF

Council of the EU. (2002). Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States. *Official Journal of the European Communities, L*(190), 1-18. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:190:0001:0018:EN:PDF

Council of the EU. (2003). Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one Member State by a third-country nationals. *Official Journal of the European Union, L*(50), 1-10. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:050:0001:0010:EN:PDF

Council of the EU. (2004). Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS). *Official Journal of the European Union, L*(213), 5-7. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004D0512:EN:NOT

Council of the EU. (2004). Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data. *Official Journal of the European Union*(L 261), 24-27. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:261:0024:0027:EN:PDF

Council of the EU. (2008). Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist . *Official Journal of the European Union, L*(218), 129-136. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0129:0136:EN:PDF

Council of the EU. (2011). *Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service.* Retrieved from The public register of Council documents: http://register.consilium.europa.eu/pdf/en/11/st10/st10093.en11.pdf

Council of the EU. (2011). *Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security.* Retrieved from The public register of Council documents: http://register.consilium.europa.eu/pdf/en/11/st18/st17434.en11.pdf

Euronews. (2010, September 23). *Italian airport security axing body scanners .* Retrieved from Euronews: http://www.euronews.com/2010/09/23/italian-airport-security-axing-body-scanners/

European Commision. (2011, December 12). *Proposal for a Regulation of the Europena Parliament and the Council - Establishing the European Border Surveillance System (EUROSUR).* Retrieved from Documentation Centre of the EC: http://ec.europa.eu/home-affairs/doc_centre/borders/docs/eurosur%20final.pdf

European Commission. (2011, November 14). *Aviation security: Commission adopts new rules on the use of security scanners at European airports.* Retrieved from Europa Press Release RAPID: http://europa.eu/rapid/press-release_IP-11-1343_en.htm

European Commission. (2011, October 25). *Communication from the Commission to the European Parliament and the Council - Smart borders - options and the way ahead.* Retrieved from Official Journal of the European Union: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0680:FIN:EN:PDF

European Parliament. (2012). *MEPs favour police access to asylum seekers' fingerprints, subject to safeguards.* Retrieved January 20, 2013, from http://www.europarl.europa.eu/news/en/pressroom: http://www.europarl.europa.eu/news/en/pressroom/content/20121214IPR04657/html/MEPs-favour-police-access-to-asylum-seekers%27-fingerprints-subject-to-safeguards

European Parliament; Council of the EU. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *The Journal of the Europena Communities, L*(281), 31-50. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:PDF

European Parliament; Council of the EU. (2000). Charter of fundamental rights of the European Union. *Official Journal of the European Communities, C* (364), 1-22. Retrieved from http://www.europarl.europa.eu/charter/pdf/text_en.pdf

European Parliament; Council of the EU. (2006). Rregulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II);. *Official Journal of the European Union, L*(381), 4-23. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:381:0004:0023:EN:PDF

European Parliament; Council of the EU. (2008). Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation). *Official Journal of the European Union, L*(218), 60-81. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0060:0081:EN:PDF

Frontex. (2010). *Ethics of Border Security.* Retrieved from Frontex: http://www.frontex.europa.eu/assets/Publications/Research/Ethics_of_Border_Security_Report.pdf

FRONTEX. (2011). *Best Practice Guidelines on the Design, Deployment and Operation of Automated Border Crossing Systems.* Retrieved January 20, 2013, from http://www.frontex.europa.eu/assets/Publications/Research/ABC_Best_Practice_Guidelines.pdf

Goldstein, J., Angeletti, R., Holzbach, M., Konrad, D., & Snijder, M. (2008). *Large-scale Biometrics Deployment in Europe: Identifying Challenges and Threats.* JRC Scientific &Technical Reports. Retrieved January 20, 2013, from http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=1899

GOV.UK. (2012, October 3). *Managing the risk to transport networks from terrorism and other crimes.* Retrieved from GOV.UK: https://www.gov.uk/government/policies/managing-the-risk-to-transport-networks-from-terrorism-and-other-crimes/supporting-pages/aviation-security

Gurzu, A. (2012, June 27). *EUROSUR: Curtailing migrants' rights or saving lives?* Retrieved from Europolitics: http://www.europolitics.info/sectorial-policies/eurosur-curtailing-migrants-rights-or-saving-lives-art338213-16.html

Hayes, B., & Vermeulen, M. (2012, June). *The EU's New Border Surveillance Initiatives.* Retrieved from Statewatch: http://www.statewatch.org/news/2012/jun/borderline.pdf

Herald Sun. (2011, September 1). *Body scanners scrapped from German airports after error-filled trial .* Retrieved from Herald Sun: http://www.heraldsun.com.au/travel/news/body-scanners-scrapped-from-german-airports-after-error-filled-trial/story-fn32891l-1226126966777

Herald Sun. (2012, August 15). *Australian airports to get body scanners.* Retrieved from Herald Sun: http://www.heraldsun.com.au/travel/news/australian-airports-to-get-body-scanners/story-fn32891l-1226450943695

Infowars. (2011, October 26). *New Trials Show Body Scanners Have Up To 40% Error Rate.* Retrieved from Infowars: http://www.infowars.com/new-trials-show-body-scanners-have-up-to-40-error-rate/

Parkin, J. (2011). The difficult road to the Schengen Information System II. *Justice and Home Affairs, CEPS Papers in Liberty and Security in Europe, CEPS Research Areas*, 1-41. Retrieved January 20, 2013, from www.ceps.eu/ceps/dld/4373/pdf

Parliament of Australia. (2012, August 12). Inquiry into the Aviation Transport Security Amendment (Screening) Bill 2012. *Bills Digest*, 1-17. Retrieved from http://parlinfo.aph.gov.au/parlInfo/download/legislation/billsdgs/1847582/upload_binary/1847582.pdf

Polish EU Presidency. (2011, July 18-19). *Informal meeting of the Justice and Home Affairs Ministers in Sopot.* Retrieved from Statewatch: http://www.statewatch.org/news/2011/jul/eu-council-informal-jha-smart-borders.pdf

Schiphol. (2012). *Security Scan at Amsterdam Airport Schiphol.* Retrieved from Airport Schiphol: http://www.schiphol.nl/Travellers/AtSchiphol/CheckinControl/SecurityChecksUponDeparture/SecurityScar

SMART. (2011-2014). *Scalable Measures for Automated Recognition Technologies - EU FP7 Collaborative project, Grant agreement no.: 261727*. Retrieved January 20, 2013, from http://www.smartsurveillance.eu

Sun, Z., Wanga, P., Vuran, M. C., Al-Rodhaan, M. A., Al-Dhelaan, A. M., & Akyildiz, I. F. (2011). BorderSense: Border patrol through advanced wireless sensor networks. *Ad Hoc Networks, 26*(4), 468-477. Retrieved from http://www.ece.gatech.edu/research/labs/bwn/papers/2011/j9.pdf

Tzanou, M. (2010). The EU as an emerging 'Surveillance Society': The function creep case study and challenges to privacy and data protection. *Vienna Journal on International Constitutional Law, 4*(3). Retrieved January 20, 2013, from http://www.internationalconstitutionallaw.net/download/d449cfc0d738b2b6f73e91cecd714fef/Tzanou.pdf

Villasenor, J. (2012, February 24). *High-Altitude Surveillance Drones: Coming to a Sky Near You.* Retrieved from Scientific American: http://blogs.scientificamerican.com/guest-blog/2012/02/24/high-altitude-surveillance-drones-coming-to-a-sky-near-you/

Watson, S. (2011, August 1). *German Authorities Reject 'Useless' Radiation Body Scanners.* Retrieved from Prisonplanet: http://www.prisonplanet.com/german-authorities-reject-useless-radiation-body-scanners.html

Whitley, E. R. (2008). A Symmetric Analysis of the Border Control Information Systems for People and Trade. *Proceedings of the 16th European Conference on Information Systems - ECIS*, (pp. 1117-1128). Galway, Ireland.

Wright, D., Friedewald, M., Gutwirth, S., Langheinrich, M., Mordini, E., Bellanova, R., . . . Bigo, D. (2010). Sorting out smart surveillance. *Computer Law & Security Review, 26*(4), 343-354. Retrieved January 20, 2013, from http://www.sciencedirect.com/science/article/pii/S0267364910000841

---

[1] Vildana Sulić Kenk is a Teaching Assistant of Electrical Engineering, currently working as a senior researcher at the Machine Vision Laboratory of the Faculty of Electrical Engineering, University of Ljubljana.

[2] Janez Križaj is a Ph.D. student in Electrical Engineering, currently working as a young researcher at the Laboratory of Artificial Perception, Systems and Cybernetics of the Faculty of Electrical Engineering, University of Ljubljana.

[3] Vitomir Štruc is an Assistant Professor of Electrical Engineering, currently working as a senior researcher and teaching assistant at the Laboratory of Artificial Perception, Systems and Cybernetics of the Faculty of Electrical Engineering, University of Ljubljana.

[4] Simon Dobrišek is an Assistant Professor of Electrical Engineering, currently working as a senior researcher and teaching assistant at the Laboratory of Artificial Perception, Systems and Cybernetics of the Faculty of Electrical Engineering, University of Ljubljana.