European ‘smart’ surveillance: What’s at stake for data protection, privacy and non-discrimination? *

Mathias Vermeulen[1] *and Rocco Bellanova*[2]

Introduction

Smart surveillance has become a buzzword among computer scientists and European policy makers. The European Commission is about to table a legislative proposal to implement a ‘smart borders package’,[3] and technology companies devote entire research programmes on smart surveillance.[4] While the term has not yet entered the research agenda of social scientists, surveillance studies scholars already work on surveillance measures that are, more or less explicitly, defined as smart.[5]

This article intends to contribute to both legal and social sciences debates surrounding the development of this so-called smart surveillance. It critically questions two relevant case studies: smart Closed Circuit Television (CCTV) systems and the European Union Passenger Name Record (EU PNR) proposal. They share relevant characteristics of smart surveillance: the EU PNR system would create a large socio-technical assemblage to collect, process and store passengers’ data to identify both known and unknown suspects of crimes, while smart CCTV cameras are intended to automatically detect abnormal behaviour and alert such behaviour to the controllers. In both cases, the emphasis is on the promise of sifting out relevant information and target the surveillance.

These projects are also of particular interest because they are still ‘works in progress’. Some of their core elements are already in use (e.g. CCTV and PNR), but

* Authors’ note: the authors thank Quirine A.M. Eijkman for her comments on a draft version of this article. This text is based on the researches done in the framework of the FP7 European Project SAPIENT: Supporting fundamental rights, Privacy and Ethics in Surveillance Technologies.

[1] Mathias Vermeulen is a research fellow at the European University Institute (Florence, Italy) and PhD candidate at the Law, Science, Technology and Society of the Vrije Universiteit Brussel (Brussels, Belgium).

[2] Rocco Bellanova is researcher at the Law, Science, Technology and Society of the Vrije Universiteit Brussel and PhD candidate at the Centre de Recherche en Science Politique of the Université Saint-Louis (Brussels, Belgium). Since March 2013, he is researcher at the Peace Research Institute Oslo (PRIO).

[3] European Commission, *Smart borders – options and the way ahead. COM(2011) 680 final*, Brussels, European Commission, 2011.

[4] See for instance IBM, IBM Smart Surveillance Research, available at: http://researcher.watson.ibm.com/researcher/view_project.php?id=139.

[5] See for instance L. Introna and D. Wood, ‘Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems’, in *Surveillance & Society*, 2004, vol. 2, no. 2/3, pp. 177-98. Beyond specific case studies, it is important to note that many authors have focused on the different forms that surveillance has historically taken, and have differently theorized their core features; cf. D. Lyon (ed.), *Theorizing Surveillance. The Panopticon and Beyond*, Devon, Willian Publishing, 2006.

their transformation into operational smart surveillance technologies is still mostly discussed at this point and not implemented on a wide scale within the EU or at EU level. Furthermore, the development of these projects generally faces criticism that is related to their fundamental rights impact, both at the political and academic level.

Therefore, these two case studies offer a concrete opportunity to analyze, first, how smart surveillance technologies are being developed, and, second, what their potential impact is on the right to privacy and data protection. The rest of this article is divided into two main sections. In the first section, we briefly present the main 'smart' features in both the PNR project and smart CCTV. In the second section, we outline the relevant privacy and data protection frameworks that would apply in the EU to these surveillance measures. Finally, in the conclusion we advance some observations regarding the peculiarity of *smart* surveillance when compared to *mass* or *targeted* surveillance.

1. *Smart* surveillance?

What exactly makes surveillance 'smart'? In this article we rely on the following definition:

> a smart surveillance system is 'capable of extracting application-specific information from captured information (be it digital images, call logs or electronic travel records) in order to generate high-level event descriptions that can ultimately be used to make automated or semi-automated decisions'.[6]

In this context, the *smartness* of surveillance can become polysemic. On the one hand, it could mean that surveillance systems are able to achieve their intended aims without being noticed by the person or the group that is monitored (and hence are much more effective at the same level of intrusiveness). On the other hand, one of the meanings of smart surveillance in a legal context could rather lie in the fact that the (use of a) surveillance technology is 'privacy-proof' and/or 'data protection-proof'.

1.1. Smart CCTV

A number of European research projects are currently developing smart surveillance systems that automatically detect user-defined 'threats' or 'abnormal behaviour' in public places. The system will alert then the CCTV operator who has to decide if any, and if so, what actions to take. As such, these smart surveillance technologies primarily aim to tackle the information overload that data controllers are subjected to by alerting them to potentially interesting

[6] D. Wright et al. 'Sorting out Smart Surveillance' in *Computer Law & Security Review,* 2010, vol. 26, no.4, p. 347. This definition has also been used as background assumption of the FP 7 EU research project SAPIENT, and further tuned in the collective Deliverable D1.1: M. Friedewald and R. Bellanova (eds.). *Smart Surveillance - State of the Art. Sapient Deliverable D1.1.* Brussels, FP7 SAPIENT Project, 2012.

information. Hereby a third function is added to the use of CCTV cameras: CCTV cameras are not only used as a deterring measure against crime or as a post-facto investigative tool, but they can also be used for preventive purposes.

Two research projects are of importance here: ADABTS (Automatic Detection of Abnormal Behaviour and Threats in crowded Spaces)[7] and INDECT (Intelligent information system supporting observation, searching and detection for security of citizens in urban environment).[8] The decision to select these projects was based on various European news reports that these projects were engaging in fundamental-rights intrusive activities.[9]

Both projects have similar goals. The ADABTS project aims to 'facilitate the protection of EU citizens, property and infrastructure against threats of terrorism, crime and riots by the automatic detection of abnormal human behaviour'.[10] On the basis of the use of 'video and acoustic sensors' ADABTS plans to create models that will enable the 'prediction of the evolution of behaviour, so that potentially threatening behaviour can be detected as it unfolds, thus enabling pro-active surveillance'.[11] INDECT's ambitious aim is to design a system that enables the 'intelligent' processing of 'all information and automatic detection of threats and recognition of abnormal behavior or violence'. It specifies that this includes the 'intelligent monitoring of objects and urban areas for the purpose of automatic detection of (potential) threats related to crime, terrorism and violent acts'.[12]

On the basis of a list of indicators of a threat or 'abnormal behaviour' the CCTV operator is alerted. Both projects stress in various forms that these indicators are provided by the end-users (the police, or a public authority) or on the basis of 'objective scientific analysis'. INDECT loosely defines 'abnormal behaviour' as behaviour which is 'potentially dangerous to society', or 'related to crime', such as 'the using of knifes or guns, or unattended luggage in public places'. This aspect of smart-surveillance seems to be less problematic, since it only tries to detect and or track potentially dangerous tools in public places. But INDECT also tries to detect potentially dangerous situations and behaviour on the basis of parameters that are set by the end-users of the project i.e police departments. After some criticism in the press and even the European

[7] For more info see www.informationsystems.foi.se/~adabts-fp7

[8] For more info see www.indect-project.eu/

[9] W. Heck, 'EU to Monitor Deviant Behavior in Fight against Terrorism', in *Der Spiegel*, 21.10.2009; I. Johnston, 'EU Funding 'Orwellian' Artificial Intelligence Plan to Monitor Public For 'Abnormal Behaviour', *The Telegraph*, 09.12.2011. See in general: B. Hayes, *'Neoconoption - the EU Security-Industrial Complex*', London, Statewatch, 2009.

[10] European Commission DG Enterprise and Industry, *Towards a More Secure Society and Increased Industrial Competitiveness - Security Research Projects under the 7th Framework Programme for Research, Security*, Brussels, European Commission, 2009, p. 6.

[11] Idem.

[12] Idem at p. 52.

Parliament,[13] INDECT was keen to point out that it did not introduce the terms 'suspicious' or 'abnormal' behaviour.[14] ADABTS identified the needs of various end-users through interviews with not only police, but also CCTV operators and security managers in airports, town centers, shopping malls, football stadia.[15] It further made an effort to identify 'objective data on abnormal behavior' based on concepts for instance from clinical psychology.[16] Distinct and visible behaviour, such as all 'whole-body behaviours (including movement about a space, excessive body gestures or gait)', were identified as well as behaviours that are 'less obvious (such as signs of stress, rapid eye movements, blinking, mumbling and perspiration)'.[17]

Both ADABTS and INDECT add microphones to CCTV cameras in order to achieve these aims. In INDECT a CCTV-operator will automatically be alerted when 'dangerous sounds' are heard, such as 'gunshots, explosions, screams, crying for help in European languages, breaking glass'.[18] One of the features of the ADABTS project is that CCTV cameras would also be able to analyze the pitch of people's voices as this might be an indicator of 'abnormal behaviour'.

ADABTS and INDECT are keen to stress that they are just 'research projects' and can in no way be held responsible for the exact application of their technologies. INDECT stresses that if EU Member States want to use this type of technology, they must comply with all relevant EU fundamental rights.[19] ADABTS has a 'legal and ethical part' of the 'user needs work package', but its legal and ethical analysis similarly only covers the legal and ethical restrictions on its tests and research-activities, and does not go dig deeper into the legal implications of the use of their new surveillance technologies. According to ADABTS, their research fits better into the category of 'scientific (visual) ethnographic or anthropological studies' rather than surveillance, since they are using video data only for research purposes and 'the immediate intention is not the prevention of crime or improvement of security'.[20]

[13] During the past two years, more than 20 written questions have been asked by Members of the European Parliament about this project in the European Parliament.

[14] J. Derkacz, and M. Leszczuk, *D0.6 INDECT – Ethical Issues – 2010.* Warsaw, Indect, 2011, p.21. (Hereafter INDECT D0.6) It states that 'in our case we clearly understand abnormal behaviour as criminal behaviour', and especially as 'behaviour related to terrorist acts, serious criminal activities (e.g.: murders, bank robberies, someone leaving the luggage in the airport with the bomb) or criminal activities in the Internet (e.g.: child pornography). We will produce the tools to avoid such situations'.

[15] H. Allberg, *ADABTS WP2 User Needs,* 12 May 2010, p. 7. (Hereafter ADABTS WP2)

[16] C. Neary et. al, *ADABTS D3.1 Abnormal Behaviour Definition*, 23 March 2011, p. 2. (Hereafter ADABTS D3.1)

[17] ADABTS D3.1, p. 6.

[18] INDECT D0.6, p. 12.

[19] Idem.

[20] ADABTS WP2, p. 68.

1.2 The EU-wide PNR system

Passenger Name Record data are unverified pieces of information provided by passengers and collected by carriers for enabling reservations and carrying out the check-in process.[21] Given their commercial purposes, PNR data contain several kinds of information, ranging from travel-related information to personal and relational data (the meals' options of the passenger, their credit card number, but also addresses and information on other passengers and travel agents).

Since the early 1990s, PNR and the airlines' reservation systems attracted the interest of law enforcement authorities, especially in the USA, where passenger data were progressively accessed by border and security agencies, in an increasingly automated way.[22] At present, PNR data are processed in the United States by the Automated Targeting System, which is a 'decision support tool [which] compares traveller, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based targeting scenarios and assessments'.[23] Currently, from a EU perspective, the transfer of EU-related PNR data to the Department of Homeland Security, and (part of) their processing, is based on and covered by an international agreement, the so-called 2012 EU/US PNR-agreement.[24]

A similar law enforcement interest in PNR data has also been growing within the European, as various proposals to create a similar system in the EU show, most recently in 2011.[25]. Beyond the official statements of the Commission, it is not clear to which extent specific member states already use PNR at a national level, and if they do so in the same scale and way as is foreseen

[21] European Commission, *Communication from the Commission. On the Global Approach to Transfers of Passenger Name Record (PNR) Data to Third Countries*, Brussels, European Commission, 2010, p. 3.

[22] Cf. R. Jacksta [US CBP], 'United States and European Union Passenger Name Record (PNR) Joint Review [PPT Presentantion]', Washington, DC [?], Department of Homeland Security, 2005, available at: https://www.eff.org/sites/default/files/filenode/foia_ats/20071107_ats02.pdf (last accessed on 21.02.13).

[23] US DHS, *Privacy Impact Assessment for the Automated Targeting System*, Washington, DC, Department of Homeland Security, 2012, p. 2.

[24] European Union - United States, *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*, Brussels/Washington [?], 2012. The 2012 EU/US PNR agreement is part of a saga of PNR agreements between the EU and the US, cf. also: P. Vagelis and P. De Hert. 'The PNR Agreement and Transatlantic Anti-Terrorism Cooperation: No Firm Human Rights Framework on Either Side of the Atlantic', in *Common Market Law Review*, 2009, vol. 46, no. 3, pp. 885-919.

[25] European Commission, *Proposal for a Council Framework Decision on the Use of Passenger Name Record (PNR) for Law Enforcement Purposes COM(2007) 654 Final*, Brussels, European Commission, 2007. European Commission, *Proposal for a Directive of the European Parliament and of the Council on the Use of Passenger Name Record Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime. COM (2011) 32 Final*, Brussels, European Commission, 2011. (Hereinafter : EU PNR proposal)

in the proposals of the Commission. Therefore, it is possible to assume that the adoption and implementation of the EU PNR proposal would be a real novelty in the EU 'surveillance landscape'.

The 2011 EU PNR proposal 'provides for the transfer by air carriers of Passenger Name Record data of passengers of international flights to and from the Member States, as well as the processing of that data, including its collection, use and retention by the Member States and its exchange between them'.[26] The purpose of the transfer and processing of PNR data is 'the prevention, detection, investigation and prosecution of terrorist offences and serious crime'.[27]

The most important part of the project resides in the competences of the so-called Passenger Information Units (PIUs) and the types of data processing that they are supposed to carry out. In particular, the very core of the EU PNR project focuses on four specific types of processing: (i) a 're-active' tracking of the connections among specific individuals and their travelling history and behavior in order to solve already committed crimes (to obtain further evidence or establish connections with other individuals); (ii) a 'real-time' processing of PNR data for monitoring purposes of known suspects (criminals or terrorists), which mainly consists of the running of PNR-data against existing databases (or watch-lists) and specific information sent to PIUs, whereby a match would allow for the identification of the *mala fide* traveller and the possibility to act at a distance to submit him/her to secondary screening; (iii) a 'pro-active' use of PNR data to unveil unknown suspects by running the data of all travellers against pre-established assessment criteria (a correlation operation).[28] Finally, (iv) the possibility to create and update assessment criteria is a crucial feature since it permits to exploit the stored data in such a way that the steady stream of newly incoming PNR can be better analyzed. This last processing operation is carried out on data that have been 'anonymised' and stored for five years,[29] so that PNR data are not only the yeast of existing databases or profiles, but they strongly contribute to the generation of a 'knowledge' that is largely disconnected from the individual passenger at the source of PNR data.

The EU PNR Commission proposal, seen from the perspective of 'smart surveillance' has three salient characteristics. First, the processing scheme for law enforcement would be fed, triggered and, to some extend, based on a commercial system. In this sense, it would be a sort of symbiotic, if not parasitic, system.[30] Second, it would enact and reinforce different surveillance logics: an *ex-post* investigation, a real-time matching against lists of 'known suspects' and a pre-emptive, *ex ante*, check. Third, to allow these different modes of

[26] EU PNR proposal, article 1(1).

[27] EU PNR proposal, article 1(2).

[28] Cf. article 4 EU PNR proposal, and its Explanatory Memorandum (pp. 3-4).

[29] Article 9(2) EU PNR proposal.

[30] Cf. R. Bellanova and D. Duez, 'A Different View on the 'Making' of European Security: The EU Passenger Name Record System as a Socio-Technical Assemblage', in *European Foreign Affairs Review*, 2012, vol. 17, Special Issue, pp. 109-24.

surveillance, the system requires the massive collection of personal (commercial) data, so that the narrowing and targeting of surveillance would be operated only at the level of data processing and not at the level of data collection.

2. Fundamental rights limits to the use of smart surveillance technologies

The potential impact of (smart) surveillance technologies in terms of fundamental rights has become an established debate in the academic and policy-making fields. In particular, most of these discussions are phrased in terms of privacy and data protection. While we acknowledge the relevance of other fundamental rights, such as the freedom of movement and due process, our article mainly focuses on privacy, data protection, and non-discrimination and in particular on their European legal conceptualizations. In this section, we analyse each project from this perspective.

2.1. Smart CCTV

On the European level the Article 29 Working Party has asserted that the principles of the Data Protection Directive apply to any information — including sound and image information — concerning 'an identified or identifiable person', by any type of surveillance technology.[31] INDECT assures that personal data such as 'the faces of persons, or care plate numbers' are anonymized through encryption. According to INDECT, this enables the CCTV-operator to review events 'without violating privacy rights'.[32] While this kind of anonymization is to be preferred from a privacy point of view, it must be noted that this type of information is still considered as personal data, since the image can be de-anonymized by a public authority for the purposes of investigating a crime for instance.[33] Furthermore, it is reasonable to assume that images would not qualify as 'personal data' if the subjects are generally not identifiable due to insufficient original image quality.

If personal data is processed, it has to be done in accordance with the national law of the country where it is used. The Article 29 Working Party points out that the data controller must be aware that certain public functions may only be exercised under the law by specific, non-administrative bodies such as, in particular, law enforcement agencies.[34] This is of importance, since the end-users of these smart surveillance technologies consist of a much bigger group than such agencies.

As regards the limitation of purposes, the deployment of these systems should first be limited to cases where alternative means and/or security measures

[31] Article 29 Data Protection Working Party, *Opinion 4/2004 on the Processing of Personal Data by Means of Video Surveillance*, Brussels, p. 15. Hereafter, Article 29 2004.)

[32] INDECT D0.6, p. 12.

[33] The Article 29 Working Party states that identificability within the meaning of the Directive may also result from matching the data with information held by third parties, or else from the application, in the individual case, of specific techniques and/or devices. Idem note 31.

[34] Article 29 2004, pp. 16-17.

prove clearly insufficient or inapplicable in view of the purposes of the processing.[35] The Article 29 Working Party has pointed out that surveillance performed on 'grounds of actual public security requirements, or else for the detection, prevention and control of criminal offences' should respect the requirements of Article 8 ECHR.[36] In particular, it points out that the use of such measures has to be proportionate 'to the prevention of concrete risks and specific offences — e.g., in premises that are exposed to such risks, or in connection with public events that are likely reasonably to result in such offences'.[37] As a matter of best practice it can be highlighted that the Italian guidelines on video surveillance point out that the use of these systems should be limited to situations where there is 'actual, proportionate requirements concerning prevention or suppression of concrete, specific dangers as impending on a good — this is the case, for instance, of premises exposed to actual dangers or events that can reasonably produce prejudicial effects'. This for instance leads this authority to conclude that 'it is unlawful to perform pervasive video surveillance of whole areas in a city — perhaps imaged in full and without intermission in the absence of adequate requirements e if the conditions referred to above are not fulfilled'.[38]

In order for the data processing to be proportionate, the collection of personal data should be limited to what is necessary to achieve the purpose for which the data are gathered and further processed. The technology used should be adequate in respect of the purposes sought, which entails a sort of 'data minimization' duty on the controller's part.[39] As such, these surveillance systems are even more targeted — or 'smarter' than 'normal' surveillance technologies.

A key feature of smart surveillance techniques is that they are used to monitor identifiable persons as they are moving in public places (or at least in publicly accessible premises). According to the Article 29 Working Party, such an individual in transit may well expect a lesser degree of privacy, 'but not expect to be deprived in full of his rights and freedoms as also related to his own private sphere and image'.[40] The European Court of Human Rights has earlier indicated that camera surveillance in public places where no visual data is recorded does not as such interfere with the individual's private life.[41] Only when materials obtained through such devices are made public in a manner or degree beyond that normally foreseeable an interference with the right to privacy can

[35] Idem, p. 18.

[36] Idem, p. 13.

[37] Idem, p. 13.

[38] As quoted in F. Coudert, 'When Video Cameras Watch and Screen: Privacy Implications of Pattern Recognition Technologies', in *Computer Law & Security Review*, 2010, vol. 26, no. 4, p. 382.

[39] Article 29 2004, p. 19.

[40] Art 29 WP 2004, p. 5

[41] European Court of Human Rights, *Perry vs United Kingdom*, 17 July 2003, §38.

occur.[42]

On the basis of these precedents it seems that the right to privacy is only triggered to the extent it protects personal data. However, it could also be argued that the use of these systems might affect underlying goals of the right to privacy such as the protection of dignity and the preservation of individual autonomy, which ensure that a person is able to exercise other fundamental rights. Freedom of expression and the right to association for instance all require privacy to be able to develop effectively.[43] Goold, for instance, stresses the political value of privacy by saying that 'without privacy, it is much harder for dissent to flourish or for democracy to remain healthy and robust'.[44] This is an important point to make since the right to privacy is quite often only described in individualistic terms, which makes it an easy target for proponents of 'balancing' privacy with the greater societal good of security. It might be argued that this political value of privacy might be affected by the abuse of smart surveillance technologies. It would not require much imagination to see the potential of such technologies for authoritarian regimes, which could use it to detect and respond to any early sign of protest.

Central to the use of smart surveillance technologies is the ability to sort one group or person from another, so that they can be treated differently. Since 9/11 there has been for instance a clear move to categorize people on the basis of the potential threat they might pose. As such, the use of these smart CCTV-systems resembles very closely so-called 'predictive data-mining', which aims to predict events based on patterns or 'classifiers' that were determined using known information.[45]

The ADABTS project has conducted research into such indicators, or classifiers for abnormal behavior or threatening activities such as fighting or pick-pocketing. According to the project there seem to exist some behavioral patterns that can indicate future abnormal and threatening behavior with 'sufficient accuracy'.[46] Nevertheless, ADABTS points out that the qualification of behavior as 'abnormal' is different for different times, locations, cultures or types of threat. [47] The behaviors extracted can also not be seen to be complete without

[42] European Court of Human Rights, *Peck v. the United Kingdom*, 28 January 2003, §62: 'to an extent which far exceeded any exposure to a passer-by or to security observation'.

[43] See the report of the United Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: M. Scheinin, *UN Doc A/HRC/13/37*, New York, 2009, at § 33.

[44] B.J. Goold, 'Surveillance and the Political Value of Privacy', in *Forum American Bar Association,* 2001, vol. 4, no. 1, p. 5.

[45] B. Schermer, 'The limits of privacy in automated profiling and data mining' in *Computer Law & Security Review*, 2011, vol. 27, p. 46.

[46] ADABTS WP02, p. 111.

[47] ADABTS D3.1, p. 20: 'Specific abnormal behaviour when focusing on terrorism can, for example, be mumbling prayers, or buying a one-way ticket at an airport. Then again, specific abnormal behaviour when focusing on pick pocketing can be a person stepping into the back of a line, leaving when standing in the middle of the line and getting in the back of the line a

'supplementary appearance indicators' — the way the person dresses for instance.[48] ADABTS contends further that the decision on the response to an actual or potential threat can only be assessed when a 'combination of abnormal behaviours, either observed together or sequentially' are perceived.[49] When the classification of a situation of a person as 'abnormal' is dependent on such a wide variety of factors, the accurate classification of situations and persons becomes extremely difficult, if not impossible. Even more, there exists a risk that the use of certain indicators can amount to discrimination by singling out individuals or social groups for adverse treatment on the basis of incorrect or misleading assumptions.[50]

Despite the fact that this Article 14 of the European Convention on Human Rights does not contain a general prohibition of discrimination[51], the existence of the 'or other status' formulation indicates that the application of this prohibition of discrimination is virtually unlimited.[52] For this non-discrimination provision to apply, a person or a group of persons needs to show that they are subject to a difference in treatment without there being an objective and reasonable justification compared to another person or a group in an analogous situation. No difference in treatment that is based exclusively or to a decisive extent on a person's ethnicity for instance would be justifiable.

However, it is also possible that apparently neutral or objective criteria, such as specific movements, are used as classifiers in smart CCTV programs, which in practice would disproportionally affect the right to privacy of individuals of a specific group. For instance, discrimination might occur if a smart CCTV-camera alerts an operator frequently on the basis of suspicious movements that are in fact linked to practicing a specific faith.

little while later'.

[48] ADABTS D 3.1, p. 6.

[49] ADABTS D 3.1, p. 2.

[50] House of Lords, *Surveillance: Citizens and the State*. London, 2009, p. 14.

[51] Article 14 of the European Convention stipulates that: [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. An additional protocol, Protocol 12, has also been drafted and has been ratified by 17 member states of the Council of Europe (Albania, Andorra, Armenia, Bosnia, Croatia, Cyprus, Finland, Georgia, Luxembourg, Montenegro, the Netherlands, Romania, San Marino, Serbia, Spain, Macedonia and Ukraine). This protocol states that 'any right set forth by law' (as opposed to the rights in the Convention) shall be secured without discrimination.

[52] Article 21(1) of the Charter of Fundamental Rights of the European Union adds explicitly that discrimination on the basis of genetic features, disability, age or sexual orientation are prohibited as well. Article 21(2) prohibits discrimination on the basis of national origin 'within the scope of application of the Treaty establishing the European Community and of the Treaty on European Union'.

2.2. The EU PNR project

Since the presentation of the first proposal in 2007, the EU PNR project has triggered several important controversies, ranging from its impact on fundamental rights to the sharing of costs and the technical architecture of data transfers.[53] In this article we focus only on some of the main points of criticism related to privacy and data protection, leaving aside important issues such as the geographical scope of the system and its potential impact on the freedom of movement within EU borders. Some points of friction deserve special attention: the respect of the purpose limitation and the data minimisation principles; the length of data retention; the introduction of a EU-wide profiling system; and the possible shift towards what some scholars have called a 'regime of suspicion'.[54]
As mentioned in the description above, the EU PNR system is largely relying on data originally collected for a commercial purpose. This creates a friction with the principle of purpose limitation, as the entire system is based on 'further processing' *vis-à-vis* the initial collection. This friction is coupled to a rather wide purpose of the system, which might result in different uses and practices among different authorities.[55] Furthermore, this form of indirect data collection is, by default and design, massive. While the proposal does not oblige air carriers to collect data that were not already collected at the moment of booking, the 19 fields of passenger information that have to be transmitted are already very comprehensive.[56] Based on the description of the main operations provided in art. 4(2) of the EU PNR proposal, all this data, whenever available, are processed. The only sort of minimization applies during the anonymization of data, as mentioned below, when some information are masked, and when PIUs erase the sensitive information that air-carriers may have transmitted. However, it is important to note that it is precisely the abundance of information contained in PNR that is presented by the Commission as the main reason to adopt such a system.[57] Hence, *de facto*, data minimization is neither applied at the moment of collection nor at the moment of processing.

Another point of friction concerns the retention period of PNR data. The EU PNR proposal foresees storing the data in two steps: an initial retention period of 30 days is followed by a subsequent five years period. The main difference is that after the first period all data should be 'anonymised', and 'all data elements which could serve to identify the passenger to whom PNR data relate shall be

[53] For a comprehensive review, cf. R. Bellanova and D. Duez, 'A Different View on the 'Making' of European Security…', pp. 116-17.

[54] Cf. F. Boehm, 'EU PNR: European Flight Passengers under General Suspicion - The Envisaged European Model of Analyzing Flight Passenger Data' in S. Gutwirth et al. (eds.), *Computers, Privacy and Data Protection: An Element of Choice*, Springer, Dordrecht, 2011, pp. 171-99.

[55] E.g. the definition provided in article 2(h) of 'serious crime' explicitly leaves a certain room of discretion to member states).

[56] The 19 fields of information are listed in the annex to the EU PNR proposal.

[57] Cf. the Explanatory Memorandum of the EU PNR proposal, and in particular the comparison with 'existing provisions in the area of the proposal', pp. 6-7.

masked out'.[58] Despite this anonymization procedure, the period of retention can be seen as both particularly long and intrusive, especially taking into account that the mere retention of data can already be considered as an interference with the right to privacy and that the vast majority of the data relates to innocent people. Furthermore, it should be noted that the 'masking out' of data is a reversible procedure, as the proposal clearly states that access to the full PNR is still possible in specific occasions and at specific conditions.[59]

One of the main elements of concern of the EU PNR system is the introduction of what might be called an 'EU-wide profiling system'. While the text of the proposal does not explicitly use the word 'profiling' (favouring the word 'assessment'), it is possible to classify some of the operations mentioned above as profiling, as they aim at processing data against patterns and thus establish correlations.[60] In particular, both the 'pro-active' use of PNR to identify unknown suspects and the elaboration of assessment criteria could be considered as profiling operations that permit to detect not yet perceived correlations. The introduction of this kind of measures could be perceived as problematic because the EU currently lacks a specific legal framework for profiling, and only relies on the application of the provisions of the European Data Protection Directive[61] and the Council Framework Decision on Data Protection on 'automated individual decisions'.[62] The perceived risks of profiling are multiple, and, in the case of a system such as the EU- PNR one, mostly concern possible discrimination, the effects of false positives and false negatives, and the difficulty to contest the adverse decisions.[63] The EU Fundamental Rights Agency has been particularly attentive to the issue of possible discrimination, underlining the potential for both direct and indirect discrimination.[64] However, compared to the first Commission

[58] Article 9.2 EU PNR proposal.

[59] Idem.

[60] A possible working definition of profiling, from a social sciences perspective, is advanced by Hildebrandt: '[t]he process of 'discovering' correlations between data in databases that can be used to identify and represent a human or nonhuman subject (individual or group) and/or the application of profiles (sets of correlated data) to individuate and represent a subject or to identify a subject as a member of a group or category', M. Hildebrandt, 'Defining Profiling: A New Type of Knowledge?', in M. Hildebrandt and S. Gutwirth (eds.), *Profiling the European Citizen. Cross Disciplinary Perspectives*, Springer, Dordrecht, 2008, p. 19.

[61] See article 15 of the Data Protection Directive.

[62] See article 7 of the Framework Decision. See also: L.A. Bygrave, 'Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling', in *Computer Law & Security Report*, 2001, vol. 17, pp. 17-24. The notion of profiling has been introduced in the legislative texts presented by the Commission in the framework of the Data Protection Reform, and it largely rely on the wording already used for 'automated individual decisions'.

[63] For a more comprehensive list of potential threats, cf. S. Gutwirth and M. Hildebrandt, 'Some Caveats on Profiling', in M. Hildebrandt and S. Gutwirth (eds.), *Profiling the European Citizen. Cross Disciplinary Perspectives*, Springer, Dordrecht, 2008, p. 34.

[64] FRA, *Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Directive on the Use of Passenger Name Record (*PNR*) Data…,* Vienna, European Union Agency for Fundamental Rights, 2011; and *Opinion of the European Union Agency for*

proposal, the 2011 EU PNR proposal provides some elements to mitigate these risks. To prevent direct discrimination, the processing of PNR data revealing sensitive information (health, ethnicity, religion…) is prohibited (art.11(3)), adverse decision should not be based on these data (art.5(6)), and sensitive data should be deleted when received by air carriers (art.11(3)). As for the risk of indirect discrimination, the EU PNR proposal includes a provision concerning the creation of statistics on both 'the number of identifications of any persons who may be involved in a terrorist offence or serious crime […] and the number of subsequent law enforcement actions that were taken involving the use of PNR data per air carrier and destination' (art.18(1)).[65] Such statistics make it possible to track the efficiency and effects of the EU PNR system, and as such these statistics constitute an important safeguard. However, it is still not clear how this provision will be translated in practice at the moment of implementation. Furthermore, the recent case of the lack of cooperation of many member states in providing statistics on the implementation and use of the Data Retention Directive shows, at best, a certain difficulty for national authorities to keep records of their use of specific systems.

Despite all the safeguards mentioned so far, all these frictions and concerns raised by the EU PNR proposal tend to coalesce around the fear of a shift towards a 'regime of suspicion'. This apprehension focuses on the use of commercial data and the symbiotic character of the entire system, which doesn't provide clear information on how this system works and what negative consequences it can result in (denial of boarding, further questioning, collection of evidence…). Surely, the 2011 EU PNR proposal responds to several data protection concerns and requirements. Nevertheless, the more general (but not less important) issue of the strict necessity and of the proportionality of a surveillance measure that implicates such a huge number of innocent people remains essential.[66] It is noteworthy that this crucial question does not only underlie the fundamental rights controversy, but it also surfaces in the debates concerning the geographical scope of the measure and the selection of the most 'threatening' air-routes.

3. Concluding remarks: is *smart* surveillance to be distinguished from *mass* or *targeted* surveillance?

According to the Oxford Dictionary the word *surveillance* was developed in the early 19th Century in France, and literally means 'watching over' something. The dictionary defines surveillance as 'close observation, especially of a suspected

Fundamental Rights on the Proposal for a Council Framework Decision on the Use of Passenger Name Record (PNR) Data for Law Enforcement Purposes, Vienna: European Union Agency for Fundamental Rights, 2008.

[65] The introduction of specific statistics as a mid-term safeguard against indirect discrimination was proposed by the Fundamental Rights Agency in its 2008 opinion.

[66] Cf. also EDPS, *Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on the Use of Passenger Name Record Data…,* Brussels, European Data Protection Supervisor, 2011, §§8-10.

spy or criminal'.[67] The Cambridge Dictionary uses a wider definition and introduces another important actor besides criminals in their definition by saying that surveillance is 'the careful watching of a person or place, especially by the police or army, because of a crime that has happened or is expected'.[68] Privacy expert Roger Clark separated the surveillance of persons in two distinct categories: *personal* and *mass* surveillance. The former refers to the surveillance of an identified person, and the latter category refers to the surveillance of a (large) group of people.[69]

How does *smart surveillance* fit into these categories? Calling a measure *smart* might raises the expectation, from a legal point of view, that a measure will be targeted to a specific individual, thereby reducing adverse effects on others. This meaning of smart also correlates with the principle of data minimization that as little as possible data should be actually gathered. Hence, data minimization should not only affect smart surveillance at the moment of data collection, but also its core data processing features, which should be able to generate knowledge out of a limited data-set. Such a possible conceptualization of smart surveillance seems particularly promising from a human rights perspective, as it would dramatically reduce its possible negative impact. However, while the Commission for instance supports this principle of data minimization in its communication on the reform of the Data Protection Directive, it nevertheless accepts that this 'smart' principle is not entirely appropriate in a law enforcement context.

Some surveillance technologies can be transformed in 'smart' ones by the adoption or inclusion of specific features. For example, smart CCTV cameras only store data when the system notices a 'dangerous' object or a dangerous 'situation'. As such, these cameras are therefore perceived as a form of tailored surveillance, in which data gathering is somehow scalable without on-going retention of data. An operator working in a CCTV control-room will only be interested in an individual when the system signals that 'something is wrong'. This leads easily into thinking that persons who don't trigger the pre-defined alerts of these smart surveillance systems won't be affected by their use, which, consequently, does not amount to an interference with their rights.

Another advantage seems to be that there is no risk of discrimination in using smart surveillance techniques, since it is the machine that selects persons for further investigation, and not an operator. In the case of smart CCTV cameras no decision with a negative effect are taken without further verification by an operator. Smart surveillance technologies only help the operator to focus his attention to persons to whom — according to the machine — might be interesting

[67] Oxford Dictionaries, '*Surveillance*', Oxford Dictionaries. Retrieved 27 November 2012 at http://oxforddictionaries.com/definition/surveillance.

[68] Cambridge Dictionaries, 'Surveillance', Cambridge University Press. Retrieved 27 November 2012 at http://dictionary.cambridge.org/dictionary/british/surveillance?q=surveillance.

[69] R. Clarke*, Introduction to Dataveillance and Information Privacy, and Definitions of Terms*. Retrieved 27 November 2012 at http://www.rogerclarke.com/DV/Intro.html.

to look further into. Preamble 20 and Article 3 (5) of the Commission's EU PNR proposal similarly provide that no enforcement action shall be taken by the PIUs and the competent authorities of the member states solely on the basis of the automated processing of PNR data.[70] In other words, smartness is performed by a re-distribution of roles between machines and human operators. Machines should ensure that the first shift is not biased by prejudices, then, the (same) human operators that were initially sidelined, are supposed to guarantee a fair judgment of the 'anomalies' spotted by machines. Such a rationality can foster the idea that surveillance by machines, which have a much greater surveilling capability compared to humans is, by default, less discriminatory, and therefore their use should be further extended in order to compensate human prejudices.

This does not mean however that no discrimination concerns arise. The idea that machines per definition enforce 'neutral' criteria is misleading. Since their 'nature' cannot be presented as a guarantee against discrimination, their operations, and their interactions with other elements, should equally be the object of a series of controls, including ex-post checks, to ensure that discrimination is not taking place. In this sense, human verification is just an instrument, and not the definitive solution. Rather, an accurate use of statistics, as proposed by the Fundamental Rights Agency in its EU PNR opinions, could prove an important step to ensure oversight on the entire surveillance process, and contribute to a proper assessment of the effectiveness and the very necessity of smart surveillance practices.

[70] A comparable provision has been included with regard to the tasks of the competent authorities in article 4(6).