Privacy by Design – The Case of Automated Border Control

Pagona Tsormpatzoudi, Diana Dimitrova, Jessica Schroers, Els Kindt

Privacy by Design – The Case of Automated Border Control

Pagona Tsormpatzoudi, Diana Dimitrova, Jessica Schroers and Els Kindt

Interdisciplinary Centre for Law & ICT/Center for Intellectual Property – KU Leuven, Belgium

{pagona.tsormpatzoudi, diana.dimitrova, jessica.schroers, els.kindt} @law.kuleuven.be

Abstract. Function creep, i.e. when the purpose specification principle is breached, is a major challenge for personal data processing operations. This is especially a clear risk in the field of Identity Management when biometric data are deployed. The concept of privacy by design, set forth in the data protection reform, could, in principle, contribute to mitigating function creep. An implementation is discussed hereunder in relation to Automated Border Control ('ABC').

Keywords: function creep; automated border control, ABC, identity management, biometric data, privacy by design, automated erasure, attribute based credentials, pseudo-identities

1 Introduction

In the era of globalization, mobility becomes fast and easy. People on touristic or professional travels flood airports, which becomes a challenge for border authorities. Automated Border Control is proposed by some as a solution. While there is no formal definition yet, ABC is understood as an automated system which performs several border control functions: travel document authentication, verification that the traveller is the rightful holder of this document, database checks, and automated verification that the entry conditions are fulfilled (FRONTEX, 2012) (European Commission, 2013).

ABC represents a new concept and trend in the technologies for external border control in the EU. External border control refers to the entry and exit checks carried out at the external borders of the Schengen Member States[1] (e.g. when one travels between Poland and Costa Rica), as the internal checks between the Schengen States have been abolished (e.g. between France and Germany). ABC in the EU is designed for people traveling internationally, which means crossing the external borders of the

[1] All EU Member States, except the UK, Ireland, Bulgaria, Romania, Cyprus, Croatia, but including 4 non-EU Member States: Iceland, Norway, Liechtenstein and Switzerland.

adfa, p. 1, 2011.

EU. External borders can be Schengen borders but also some EU non-Schengen borders, e.g. UK. While national ABCs are different from one another and are currently primarily used by EU/EEA/CH citizens, proposals are being made to allow certain Third-Country Nationals to use it as well (see Smart Borders Package). Thus, the future might bring an increasing number of travellers from all over the world using ABC.

At the same time, the amount of existing and available data has globally exploded. This amount of data is often too big to be traditionally managed and from this factor the notion of Big Data emerged. Viktor Mayer-Schöneberger and Kenneth Cukier describe Big Data as "things one can do at a large scale that cannot be done at a smaller scale" which could change the relationship between citizens and governments (Mayer-Schöneberger & Cukier, 2013). What is special about this, is that Big Data is the "technique to mine relevant patterns from stored or even streaming data" (Hildebrandt, 2013). A common criticism with regard to big data is that much information is collected to the largest possible amount whereas the patterns emerging from it will determine how data will be used later (Andrejevic, 2014). The use of big data analytics can bring a lot of advantages, since their claimed main potential is "the ability to uncover new purposes in the data which may create a win-win situation" (Hildebrandt, 2013). However, Big Data might also give rise to function creep, as it might enable data processing activities for purposes not foreseen when the data was initially collected.

In such a context and taking into account the opportunities that emerging technologies, such as ABC, are able to offer, traveller data is often of interest for law enforcement. Even though crossing the border is related to the protection of public and national security, the act of crossing a border is not registered and is not a criminal act per se. Thus, in general, the processing of personal data in a border control context and subsequently by ABC falls within the Directive 95/46/EC soon to be replaced by the proposed General Data Protection Regulation.[2] Therefore, the purpose specification principle of article 6(1) b of the Directive applies and has to be considered in the case of ABC. Hence, the purpose should be clearly defined and personal data, especially biometric data, when used, for example for border control purposes, should not be further processed in ways incompatible with those purposes.

The same Directive 95/46/EC provides in article 13 for derogations on different grounds that provide the possibility to deviate from the principle of purpose specification, for example, in case of the prevention of criminal offences, national and public security on a case-by-case basis and when safeguards are put in place.

In this paper, we first examine ABC as an identity management application and its risks. We present the specificities of ABC as a new trend in border control, and we dive into the concept and factors that trigger function creep (Section 2). Later on, we explore the potential of the concept of Privacy by Design to present some measures for privacy-preserving. ABC, by proposing certain privacy enhancing technologies as

2 The data processed by the Schengen Information System II (Council Decision 2007/533/JHA) on wanted persons and objects, consulted occasionally when EU/EEA/CH cross external borders of the EU, is not subject to Directive 95/46/EC.

viable technical applications (Section 3). Finally, we conclude that Privacy by Design is an approach which certainly offers many advantages but that the peculiarities of certain applications, such as ABC, require particular attention and further specifications (Section 4).

2 From manual to Automated Border Control: new trend, new challenges

2.1 ABC as a new trend in border control

The number of e-Gates[3] and national ABC programmes throughout the EU has been growing (e.g. No-Q and PRIVIUM in the Netherlands; PARAFE in France).[4] Depending on the national implementation, some systems rely on prior registration into a programme. Other systems do not require a prior registration and they are based on verification of the facial or fingerprint image against the chip of the EU biometric passport.

Currently, border checks are regulated by the Schengen Borders Code (SBC). The SBC, however, does not constitute a sufficient legal basis for ABC, as it regulates the process as carried out by border guards, not by self-service e-Gates (article 7 and 15 SBC). To solve the problem of the missing legal basis, national authorities either amended their national laws or used article 7 of Directive 95/46/EC. Those national ABC programmes that rely on consent (article 7 a), must ensure that consent is informed and freely given (article 2 h). Travellers must be informed about how, why and by whom their data are going to be processed and how they can exercise their rights as data subjects. In addition, consent implies a voluntary act, which requires the existence of a viable alternative (Art. 29 WP, 2012), i.e. a real opportunity to choose between ABC and manual border control.

We will examine the case of automation of the manual border checks for EU/EEA/CH citizens; in case of Third-Country Nationals the process is more complex.

---

3 Although the e-Gates in the EU differ in their design and functionality, in general terms they refer to an electronic gate where the border control check is carried out in a self-service manner by the travellers themselves. Normally it is equipped with a travel document reading device and a device for biometric scanning and verification or identification and is connected to the relevant background systems (e.g. for wanted individuals, such as the Schengen Information System II).

4 The enumerated programmes are national ABC programmes introduced by the individual Member States and exemplify different implementations of ABC. While both PRIVIUM and PARAFE require a prior registration, in the case of PRIVIUM the biometric data (iris) is stored on a smart card, while in PARAFE the biometrics (fingerprints) are stored on a central database (French citizens do not need to register). No-Q, on the other hand, does not require pre-registration.

2.2 ABC as Identity Management Application

Identity management at the Schengen borders raises the issue of trust. The Schengen Member States must ensure that the used token(s) and identifier(s) to claim/verify traveller identity are reliable, and not fake, forged, or stolen. Passports are in general considered to provide reliable identification although they can still be counterfeit or forged. In order to maintain this high level of trust between Schengen Member States, ABC proponents propose biometric processing for verification and/or identification purposes, as biometrics are considered to be a reliable link between travellers and their travel documents or the biometric data stored on a database for registered travellers. Biometric-based ABC hence changes the nature of identity management at borders, e.g. the method of registration and authentication. This raises privacy and data protection concerns as will be examined below.

The border control process can be split in the several steps of an Identity Management process. While there are numerous approaches to Identity Management, the two basic steps are always registration and authentication.[5]

Registration. The first step is the enrolment/registration. In case of border crossing the identity provider is the national issuing governmental authority of the traveller's home country. This authority verifies that the traveller is registered as citizen and issues a token (usually a passport). In addition to personal information like nationality and name, the passport contains a facial image of the person and his/her fingerprints as identifiers on the chip of the passport. These tokens can be used for both manual and automated border control, but in the case of a Registered Traveller Programme ("RTP"), a separate pre-registration is necessary to use the system.[6] Currently, there are different national implementations of RTPs across the EU and the processes are not harmonized (e.g. PARAFE in France and PRIVIUM in the Netherlands). Generally, for registration in RTPs, first the identity of the traveller needs to be verified with the passport. Then it is examined that the traveller fulfils the entry requirements. Afterwards the identity is registered in the database and linked to the biometric identifiers of the traveller. These biometric identifiers could be stored either on a central database (e.g. PARAFE) or on a separate token, like a card (e.g. PRIVIUM).

5 For example: OECD, Digital Identity Management: Enabling Innovation and Trust in the Internet Economy, 2011, describes registration, authorization, authentication, access control and revocation as IdM processes. A. Jøsang divides IdM in the Registration -, Operation - and Termination phase: Identity management and trusted interaction in Internet and mobile computing, IET Information Security, 2014, 8/2, p. 71.

6 For example, the European Commission has tabled a proposal for a Registered Traveller Programme that would apply to some Third Country Nationals, who fulfill certain requirements. It is part of the Smart Borders Package, which is currently subject to a feasibility test (study and pilot). As it concerns Third Country Nationals and not EU/EEA/CH citizens, the proposal is outside the scope of this paper. See Proposal for a Regulation of the European Parliament and of the Council establishing a Registered Traveller Programme, COM (2013) 97 final, Brussels, 28.2.2013.

Authentication. Authentication is the process of verifying the claimed identity of a user (OECD, 2007). Border control in general seeks to address three issues: whether the passport (1) is valid and authentic, (2) has not been stolen, lost or misappropriated (and therefore has been revoked), and (3) that it belongs to the person presenting it (Article 7(2) SBC). In order to establish the link between the person presenting the identifier and the identifier itself, sometimes an additional verifier is used. A verifier is an attribute which is somehow hard to produce or a secret between the system and the user (Wayman, 2008). In ABC biometrics are used as verifier or identifier as it is claimed to be more secure and trusted.

The ABC systems which do not make use of pre-registration can only make use of biometric data already included in the travel document. Usually this is done with a 1:1 comparison, comparing, for example the face of the traveller automatically against the data in the passport. Since the verification is done by comparing the information on the chip of the passport, in principle no registration or data base of the biometric data is needed. But the possibility that the information presented is retained after automated verification to build a database or the information is to be checked with other databases cannot be ruled out, unless appropriate measures are taken to prevent this.

RTPs are not restricted to the information on the passport and can make use of additional biometric and alphanumeric data. The authentication can take place in three ways: i. the biometric identifier is registered in a database and then becomes the only identifier of the traveller in a 1:n comparison against all biometrics in the database, ii. the biometric information in the database is linked to a key which the traveller gets in order to open the database and perform a 1:1 verification, or iii. the registered traveller gets a token (e.g. a smartcard) with the biometric identifier for a 1:1 verification against the token.

2.3 Function creep as a risk of ABC

Automated Border Control changes the nature of identity verification at external borders through the automated processing of biometrics during the check. During the manual check, the border guard visually compares the facial image on the passport with the persona standing in front of him. However, in the ABC process, the verification is automated, i.e. the biometrics on the chip of the passport are verified against the live image. Article 29 WP recognized that the deployment of biometrics poses specific data protection and privacy challenges, due to its sensitive nature and thus their processing should be examined, inter alia, in light of the purpose for which they are processed (Art.29 WP, 2013).

Nevertheless the processing of biometric data in ABCs raises, amongst other legal concerns,[7] privacy and data protection risks. One of these risks is the problem of func-

7 Another relevant legal concern is, for instance, the question of legality – on what occasions is the comparison of live fingerprints against the chip of the passport allowed (cfr. Opinion of Advocate General in the case of Schwarz (Curia, 2013). According to the Advocate General, the fingerprints of EU citizens are to be verified when there is a suspicion as to the whether the passport belongs to the one presenting it but this is at present not officially decided.

tion creep. Function creep refers to the "gradual widening of the use of a system or database beyond the purpose for which it was originally intended" (EDPS, 2012, p. 7). This entails the risk that the new usage of the data might have a more severe effect on the rights of data subjects than the initially planned usage (EDPS, 2012) (Lodge, 2010). In addition, since the incompatible usage of data would violate the purpose limitation principle (EDPS, 2012) (EDPS, 2006), this could result in an "erosion" of all other related data protection principles by using already available data beyond the purposes for which they were originally collected (Art.29 WP, 2013).

In the context of ABC, function creep could emerge as a result of several factors. These factors could be central storage of (biometric) data in databases if registered traveller databases are created or data from the e-Gates is not deleted and technical interoperability between different databases. This in turn enables the re-use of the already stored data for incompatible purposes, e.g. law enforcement.

Central Storage. Creation of central databases which store biometric identifiers of travellers is one important factor enabling function creep, as it facilitates the later use of them for further purposes, such as law-enforcement purposes. The core issue is that the biometric data, when stored centrally, are not under the control of the traveller, and thus he or she cannot effectively determine their use and re-use. This is especially problematic in the case of biometric data, which are unique and irreplaceable, in contrast to PINs and passwords. Thus, their misuse could have severe consequences for individuals. Central databases can be established in the framework of an RTP or when live biometric data are presented at the border only for verification purposes, but they are stored for later, instead of being deleted as soon as the traveller crosses the border. In addition, the storing of any personal data of EU/EEA/CH citizens using ABC technology challenges the Union right to freedom of movement, as it provides the opportunity to track their movements in and out of the Schengen area and there is currently no legal basis to track the entry and exit of EU/EEA/CH citizens.

Interoperability. Once databases are created, technological interoperability enables interlinkages between them. This blurs the functional separation between databases created for different purposes. Data from different databases, e.g. national and European databases[8] used for border control, are cross-matched with each other or even with other databases, not used for border control purposes such as law enforcement databases.[9] From the combined information further knowledge about travellers can be

8 The databases meant here, in the context of EU citizens, are the Schengen Information System ("SIS II"), which can store facial images and fingerprints, relevant national databases which can contain biometric data, as well as national RTP programmes, such as PARAFE in France.

9 E.g. a database of registered travellers is cross-matched against a police database on wanted criminals.

derived, which is enabled with big data analytics (Rubinstein, 2013).[10] This is further facilitated by the usage of biometric identifiers, which can serve as the primary key to these databases (Kindt, 2013). In this way biometrics can become universal identifiers, instead of every database producing its own unique identifier. For example, the live biometric may be presented for verification at e-Gates and at the same time may be used to search national and European databases in real time with little effort.

Re-use of data for law-enforcement purposes. The breach of the purpose limitation principle could lead to a function creep and potentially have a negative impact on individuals, in a sense that storage and cross-matching of data might enable re-use of data in a way that it can be used against travellers.

ABC processes automatically (biometric) data of the travellers who use it. The majority of these travellers are presumably innocent individuals. Saving and cross-checking their data on a systematic basis with law-enforcement databases would be disproportionate, as EU/EEA/CH citizens should be checked in criminal databases such as SIS II only on a non-systematic basis (article 7 (2) Schengen Borders Code). Thus there is no legal basis for checking whether all EU/EEA/CH travellers that use ABCs are in some way suspects, under investigation, etc. That is why it is important to keep the functional separation between databases.

Such further usage of biometric data, e.g. for law-enforcement purposes, when not regulated by a law which enshrines sufficient safeguards for data subjects, could create a legal vacuum and place in effect all travellers under general suspicion without a sufficient level of protection for their rights. An illustrative example is a potentially false hit of the fingerprints of a registered traveller against a law-enforcement database and subsequent proceedings against the individual. Access to law-enforcement authorities has already been granted in the case of EURODAC, which was not initially envisaged in the original Regulation. Thus, the purpose of EURODAC was extended from regulating the asylum application process to law-enforcement, without sufficient corresponding safeguards to individuals, as the EDPS criticized the Commission Proposals of 2008, 2009 and 2012 to extend access to the data for law- enforcement purposes (EDPS, 2012). EURODAC was officially amended anyway to grant access to law-enforcement authorities ((Official Journal of the European Union, 2013). The Visa Information System (VIS) was also amended to allow access to law-enforcement authorities (Council, 13.8.2008). When the access by law-enforcement authorities is not clearly regulated, including the consequences on individuals of such access, as well as measures to prevent arbitrariness and to allow individuals to exercise their rights, a legal vacuum emerges. Thus, the issue of legal vacuum, which can be observed also in ABC, is another factor which has to be taken into account when considering function creep. (Kindt, 2013) (CBP, 30.03.2007).

The issue of access by law-enforcement authorities to data processed via ABC, if such access is deemed to be necessary to be granted in the first place, has to be clearly regulated in law as the authorities cannot evoke randomly article 13 Directive

[10] Rubinstein refers to Big Data as the "… more powerful version of knowledge discovery in databases or data mining, which has been defined as 'the non-trivial extraction of implicit, previously unknown, and potentially useful info from data".

95/46/EC. It is important to bear in mind that article 13 requires a legislative measure before a derogation is applied and this measure should be justified under article 8 ECHR (CURIA, 2003).

For the reasons above, a law regulating the access of law enforcement authorities to ABC data should be adopted. This law should contain sufficient safeguards for individuals. In practice, any restriction of the rights of travellers or any re-use of their data for purposes such as security must be carefully assessed and only applied on a case by case basis.

3 Is Privacy by Design a solution?

To address function creep triggered by applications employing biometrics in the field of ABC, one should consider relevant legal, technical and organisational measures. A concept that promises tremendous benefits to the way relevant measures should be implemented is Privacy by Design.

Privacy by Design is an approach to privacy that helps enforce the privacy rules and ensures that new technologies, products or services do not create new privacy concerns but protect individuals' privacy. Its quintessence is to identify and mitigate privacy risks from the very beginning, when the means for the processing of data are determined and throughout the lifecycle of the processing (Alvaro, 2012). It is often argued that Privacy by Design is about using technology as a regulatory instrument and thus has been referred to as "code as code" or "techno-regulation" (Lessig, 2000) (Koops, Bodea, Hoepman, Leenes, & Vedder, 2009).

However, in this paper, Privacy by Design is not perceived just as a general requirement for system developers to embed as many data protection requirements as possible in the design of the system, in a sense of strictly automating compliance with the legal framework (Koops & Leenes, 2013). Rather, privacy by design is understood as a whole mind-set which embodies the idea to respect privacy at technical and organisational level (Koops & Leenes, 2013). This means that privacy should be reflected in the culture of an organisation and drive choices regarding technical design and data processing as well as strategy development and top-level decisions.

In order to unveil Privacy by Design and understand its implications in the context of ABC we first consider its development. Further, we discuss certain Privacy by Design technical applications in light of their potential to address the challenges attached to the use of biometrics without undermining the need for security of the ABC process. Special attention is given to the ISO/IEC 24745, from which we finally derive prerequisites to specify Privacy by Design.

3.1 Development of the concept

The concept of Privacy by Design is not explicitly included in the Directive 95/46/EC. However, the intention of the legislator to enforce privacy and data protec-

tion principles through technology is clear, since it provided that the data controller has to take technical and organizational measures both at the stage of the design of the system as well as at the time of the processing of personal data[11]. While legal and administrative instruments have been exhausted on policy development and monitoring, the introduction and elaboration on Privacy Enhancing Technologies have been an alternative approach to implement Privacy by Design (Koorn, van Gilsm, ter Hart, Overbook, & Borking, 2004). Privacy Enhancing Technologies have extensively been developed in relation to two data protection principles: data quality (article 6 Directive 95/46/EC) that includes both the principles of fairness and of data minimization and data security (article 17 Directive 95/46/EC). Departing from Privacy Enhancing Technologies, it was illustrated that privacy-aware design cannot be seen independently from other processes that are related to organisational aspects (Cavoukian, 2011) (Koorn, van Gilsm, ter Hart, Overbook, & Borking, 2004). Besides technologies, privacy should, therefore, have an impact on the border control processes as well as on border authorities' attitude towards privacy concerns raised by data processing activities.

Within the preparatory work for the data protection reform, both the Article 29 WP and the EDPS expressed the opinion that Privacy by Design should be recognised as a general principle and has to be articulated in provisions of specific legal instruments (Cavoukian, 2010) (Art. 29 WP, 2009) (EDPS, 2010), as an extension of the current rules on organizational and technical security measures and the general principle of accountability (EDPS, 2010). The recent Proposal for a Draft General Data Protection Regulation (European Commission, 2012), refers to data protection by design (article 23). Following the Parliament discussions, data protection by design requires that privacy should be embedded within the entire life cycle of the technology, from very early design stage, right through to its ultimate deployment, use and final disposal[12]. The Council in its report of 3rd October 2014 deleted this definition. The new Recital 61, as proposed by the Council, reads: "In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default. Such measures could consist inter alia of minimising the processing of personal data, (…) pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features"(Council of the EU, 3rd October 2014).

[11] Recital 46 and article 17 of Directive 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 (OJ L 281 31).

[12] Recital 61 of the European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

3.2 Applications

Automated erasure. Automated erasure is a Privacy by Design routine that can potentially fulfil the procedural safeguards mentioned in article 23 of the Draft General Data Protection Regulation, regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data. It can be perceived as an expression of data minimization, as deriving from article 6.1(b) and (c) of Directive 95/46/EC. It requires from the data controller not to collect more personal data than what is absolutely adequate, appropriate and necessary in order to accomplish a specified purpose. In that sense automated erasure can take several forms, including installing in the system data self-destructing mechanisms (Mayer-Schönberger, 2009)(Art. 29 WP, 2012). In light of the opportunities often arising from big data analytics (Polonetsky, 2012), which for example could be useful to enhance the functionalities of the system, automated erasure should be applied on the basis of proportionality. Storing and analysing huge data sets of travellers might enhance the security functionalities of the system but would not be necessary provided that security measures already exist at the airports. In the case of ABC, data processing involves not only alphanumeric but also biometric data, which have recently been included in the special categories of data under article 9 of the Draft General Data Protection Regulation. The fact that this sensitive data could be useful for general security purposes does not overweight the privacy risks that might emerge from such operations. It should be noted that security mechanisms are already in place, such as general surveillance measures in the airports as well as criminal law enforcement data bases. Thus a reuse of sensitive data under the excuse that they are intended to overcome security concerns would be unnecessary.

In an ABC context, automated erasure could be embedded at the stages of registration and authentication. As to the stage of registration, it is a privacy enhancement that can be achieved by not storing, i.e. erasing automatically, the original image of the biometric characteristic or any other intermediate data between the extraction steps and the (protected) template (Kindt, 2010). In this way any unprotected captured data are deleted automatically in order to prevent their misuse and mismanagement (Art. 29 WP, 2012). At the stage of authentication, any stored biometric data shall be used only for the purposes of border control and therefore should be automatically erased after the transaction with the ABC technology. They further should not be retained for longer than necessary to accomplish their intended purpose (EDPS, 2010). Other data, such as time and place of crossing, data from the biometric passport, etc., should be deleted as well, unless storage is required by law.

Use of Attribute-based Credentials for ABC? The use of Attribute-based Credentials is a Privacy by Design technique which decouples the process of identification from the process of authentication in an Identity Management system. Attribute-based Credentials are cryptographically secured carriers of properties for a particular individual and allow authentication on the basis of certain required attributes that are necessary for ABC (Jacobs & Alpár, 2013).

As described in section 2, the Schengen Borders Code provides the requirement of article 7 (2) of the Schengen Border Code to conduct minimum checks to establish identities on the basis of a travel document. Additionally the article provides that on a non-systematic basis, border guards may consult national and European databases in order to ensure that EU/EEA/CH travellers do not represent a threat to the Member State.

Applying attribute-based credentials to ABC would mean in practice that the traveller would be issued in advance with a token on which certain hashed personal data are stored. The hashed attributes could represent names, passport number and country code, expiration date of the passport and age of the traveller. This could be useful to establish whether the traveller is eligible to use the ABC by confirming he has an EU/EEA/CH nationality, is above 18 and his passport has not expired yet.

Nevertheless, to establish the identity and carry out the accompanying checks as required by the SBC, the actual personal data of the traveller would be needed.

For the establishment of identities, the names, sex, passport number and issuing authority, date of birth and expiration date of the passport are required.

Further, to search the SIS II and relevant national databases on alerts for lost, stolen, misappropriated and invalidated documents, border guards need at least the passport number and country code, but could also use names, date of birth, sex, etc.

The above-mentioned personal data are also needed to search these databases for alerts on persons (non-systematically).

For these reasons, the attribute-based credentials may not be a workable solution for ABC. However, if in principle a specific law regarding ABC would be introduced, information minimizing techniques such as attribute-based credentials could possibly be taken into account in the wording of the legislation. In such a case, the inherent loss of usable/searchable information due to the use of such a technique would be expected to face opposition from the side of the border guards.

Pseudonymous biometric identities. Function creep stemming from the factors attached to biometric authentication in the context of ABC could possibly be further addressed with pseudonymous biometric identities. Pseudonymous biometric identities , sometimes also referred to as ‘pseudo-identities’, as a generic framework for existing biometric template protection techniques, propose an architecture, which does not reveal any information permitting retrieval of the original biometric data of its owner by any person besides the enrolled data subject. In this sense, they are diversifiable, protected identity verification strings within a predefined context (i.e. the protected biometric ecosystem) (Breebaart, Busch, Grave, & Kindt, 2008).

Pseudonymous biometric identities are able to materialize biometric authentication for ABC in a privacy-respecting way. They allow storage of information which is able to perform biometric verification. As pseudonymous biometric identities represent a solution which focuses on biometric and not on alphanumeric data, it is still possible to establish the identity of the traveller on the basis of biometrics and to search the relevant databases with alphanumeric data. They can ensure data minimization and secure processing of biometric data according to Directive 96/45/EC. Further, they are able to address the requirements for the protection of biometric information posed by

ISO/IEC 24745, as described below, since they are irreversible, unlinkable and revocable.

These requirements for the protection of biometric identifiers are:

Irreversibility of the biometric identities: It calls for transformation of the biometric data in such a form that the stored biometric information cannot be reversed to the initially captured biometric data. The fact that a system is not able to trace back the data subject significantly eliminates the possibilities for misuse and mismanagement of biometric data. Subsequently function creep, which could take place in case of law enforcement access to biometric data of travellers that were collected for the purposes of border control, is avoided. Irreversibility seems however hard to achieve.

Unlinkability of the biometric identities: It prevents comparison of the biometric information with other databases or applications and calls for random generation of cancellable identifiers (Kindt, 2013). Implementing this requirement would not allow further reuse of biometric data for cross-linkages between interoperable databases, such as data stored for border control purposes and for example national (law enforcement) databases. Pseudonymous biometric identities can be renewed and diversified; multiple independent protected templates can derive from the same biometric data in order to allow travellers' authentication that cannot be linked with previous ones (Breebaart, Busch, Grave, & Kindt, 2008). Even though interoperability of databases is generally associated with function creep, use of pseudonymous biometric identities do not allow linking data subjects across databases, for surveillance purposes or across applications of the law enforcement systems.

Revocability of the biometric identities: This requirement allows that the data subject or the data controller request revocation. This would be useful in case of data breach or of function creep occurring as a result of excessive failures of the ABC or because a traveller does not wish to participate to the ABC system anymore.

Finally, pseudonymous biometric identities are universal and flexible, as they can support combinations of biometric modalities in any architecture for ABC and can be integrated in existing verification methods (Breebaart, Busch, Grave, & Kindt, 2008); i.e. two-factor verification with passport and biometric.

4 Conclusions

With the examples of automated erasure and pseudonymous biometric identities we illustrated that Privacy by Design offers promising solutions for ABC to handle identity verification based on biometric information in a privacy friendly way. In the event that the proposed reform data protection package comes into force, it will certainly foster privacy risk management through provisions such as the one on Privacy by Design. The obligation to implement a principle which proposes proactive embedding of privacy into systems design is expected to reduce the leeway for misuse and mismanagement of biometric data in the context of ABC.

As it has been particularly illustrated in the case of pseudonymous biometric identifiers, Privacy by Design could be inspired by technical standards in applications employing biometrics, as for instance the ISO/IEC 24745:2011, on biometric information protection (ISO/IEC, 2011). We support the idea that implementation of the requirements for biometric template protection would satisfy the requirement for building privacy into the design of the system, as Privacy by Design stipulates.

As it has been shown, to mitigate the risks of function creep in ABC, Privacy by Design should be approached in a holistic way and namely with technical, organisational and legal measures. Guidelines or specific legal measures should be developed in order to respond to the particularities of crucial Identity Management applications, as ABC. In addition, further legislative measures such as a proper legal basis for ABC, defining clearly the purpose, scope and functionalities of ABC, including safeguards for travellers, should be taken. Finally, as in the case of all legal principles, while Privacy by Design calls for safeguards that can enhance data protection at the e-Gates and kiosks, the question for actual implementation through enforcement remains.

Acknowledgements. This paper has been partially funded by the European Commission FP7 projects PRIPARE (PReparing Industry to Privacy-by-design by supporting its Application in Research) under Grant Agreement n° No: 610613, FastPass (A harmonized, modular reference system for all European automated border crossing points) under Grant Agreement No: 312583 and FutureID (Shaping the Future of Electronic Identity) under Grant Agreement No: 318424.

References

1. Court of Justice of the European Union, *Österreichischer Rundfunk*, C-465/00, 138/01, 139/0, 2003.
2. Court of Justice of the European Union, *Schwarz*, C – 291/12, 2013.
3. Alvaro, A. (2012). Lifecycle Data Protection Management: A Contribution on how to adjust the European Data Protection to the Needs of the 21st Century. *Privacy&Compliance 02-06/2013*.
4. Andrejevic, M. (2014). Surveillance in the Big Data Era. In K. Pimple, *Emerging Pervasive Information and Communication Technologies (PICT) - Ethical Challenges, opportunities and safeguards.* Springer.
5. Art. 29 WP. (2009). *Art. 29 Working Party - The Future of Privacy - Joint Contribution to the Consultation to the European Commission on the legal framework for the fundamental right to protection of personal data (WP168).*
6. Art. 29 WP. (2012). *Art. 29 Working Party - Opinion 3/2012 on Development in Biometric Technologies 00720/12/EN (WP193).*
7. Breebaart, J., Busch, C., Grave, J., & Kindt, E. (2008). A Reference Architecture for Biometric; Template Protection based on Pseudo Identities. *Gesellschaft für Informatik (GI): BIOSIG 2008. Proceedings of the Special*

Interest Group on Biometrics and Electronic Signatures (pp. 25-37). Bonn: Gesellschaft für Informatik.

8. Camenisch, J., Krontiris, I., Lehmann, A., Neven, G., Paquin, C., Rannenberg, K., et al. (2011). *ABC4Trust D2.1 Architecture for Attribute-based Credential Technologies.*
9. Cavoukian, A. (2010). *Resolution of Privacy by Design.* Jerusalem: 32nd International Conference of Data Protection and Privacy Commissioners.
10. Cavoukian, A. (2011). *Privacy by Design: The 7 Foundational Principles.* Information and Privacy Commissioner of Ontario.
11. CBP. (30.03.2007). *College Bescherming van Persoonsgegevens Wijziging Paspoortwet advies z 2007-00010 (invoering biometrie).* http://www.cbpweb.nl/downloads_adv/z2007-00010.pdf.
12. Council of the European Union, 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 offences and of other serious criminal offences, O.J. L 218.
13. Council of the EU, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [First reading] - Chapter IV, 3rd October 2014
14. EDPS. (2006). *Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision concerning access for consultation of the VIS by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention.* OJ 2006/C97/03.
15. EDPS. (2010). *Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy* . OJ C280/01.
16. EDPS. (2012). *Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No […/…] […..] (Recast version).* https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-09-05_EURODAC_EN.pdf.
17. EDPS. (n.d.). *Data minimisation*. Retrieved May 5, 2014, from Glossary: https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/74
18. European Commission. (2012). *Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) 25.1.2012 COM(2012) 11 final.*
19. European Commission. (28.02.2013). *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 562/2006 as regards the use of the Entry/Exit System (EES) and the Registered Traveller Programme (RTP), COM (2013) 96 final*.

20. European Commission, Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of Eurodac for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, O.J. L 180/1-30.
21. FRONTEX. (31.08.2012). *"Best Practice Operational Guidelines for Automated Border Control (ABC) Systems"*.
22. Hildebrandt, M. (2013). Slaves to Big Data. Or Are We? *IDP. REVISTA DE INTERNET, DERECHO Y POLÍTICA*.
23. ISO/IEC. (2011). *ISO/IEC 24745/2011, Information Technology - Security Techniques - Biometric Information Protection.*
24. Jacobs, B., & Alpár, G. (2013). Credential Design in Attribute-Based Identity Management. *3rd TILTing Perspectives Conference*, (pp. 189-204). Tilburg.
25. Kindt, E. (2010). The Use of Privacy Enhaning Technologies. In P. D.-H. Michelle Bezzi, *Privacy and Identity Management for Life: 5th IFIP W P9.2*.
26. Kindt, E. (2013). Best Practices for Privacy and Data Protection for the Processing of Biometric Data . In P. Campisi, *Security and Privacy in Biometrics.* London: Springer.
27. Kindt, E. (2013). *Privacy and Data Protection Issues of Biometric Applications: A comparative legal analysis.* Springer.
28. Koops, B.-J., Bodea, G., Hoepman, J.-H., Leenes, R., & Vedder, A. (2009). *D3.4 Code as Code Assessment.* VIRTUOSO FP7 project.
29. Koorn, R., van Gilsm, H., ter Hart, J., Overbook, P., & Borking, J. (2004). *Privacy Enhancing Technologies: White Paper for Decision-Makers.* Ministry of Interior and Kingdom Relation, Directorate of Public Secotr Innovation and Information Policy.
30. Leenes, R., & Koops, B.-J. (2013). Privacy Regulation cannot be hardcoded. A Critical Comment on the 'Privacy by Design' Provision in Data Protection Law. *International Review of Law, Computers and Technology*.
31. Lessig, L. (2000). *Code and Other Laws of Cyberspace.* Basic Books.
32. Lodge, J. (2010). *Biometrics in Europe: inventory on politico-legal priorities in EU27.* Best Network Deliverable D 7.1.
33. Mayer-Schönberger, V. (2009). *Delete: The Virtue of Forgetting in the Digital Age.* Princeton University Press.
34. Mayer-Schöneberger, V., & Cukier, K. (2013). *Big Data - A Revolution that will transform how we live, work, and think.* New York.

35. OECD. (2007). *Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication.* OECD.
36. Polonetsky, O. T. (2012). Privacy in the Age of Big Data: Time for Big Decisions. *Stanford Law Review*.
37. Ronald Koorn, H. v. (2004). *Privacy Enhancing Technologies: White Paper for Decision-Makers* . Ministry of Interior and Kingdom Relations, Directorate of Public Sector .
38. Rubinstein, I. (2013). Big Data: The End of Privacy or a New Beginning. *International Data Privacy Law*, Vol. 3, No.2, p. 74.
39. Wayman, J. (2008, March/April). Biometrics in Identity Management Systems. *IEEE Security & Privacy*.