Using technology to draw borders: fundamental rights for the Smart Borders initiative

Maegan Hendow, Alina Cibea and Albert Kraler
Research Department, International Centre for Migration Policy Development, Vienna, Austria

Received 20 March 2014
Revised 20 March 2014
Accepted 9 October 2014

Abstract

Purpose – This paper aims to examine the primary fundamental rights concerns related to biometrics and their use in automated border controls (ABCs), as well as how these issues converge in the European Commission's Smart Borders proposal.

Design/methodology/approach – This paper draws on extensive background research and qualitative in-depth interviews conducted in 2013 for the European Union (EU) FP-7 project "FastPass – A harmonized, modular reference system for all European automatic border crossing points".

Findings – The Smart Borders proposal not only compounds the individual concerns related to the use of biometrics in border controls and automatisation thereof, but also has serious issues of its own, premier among which is the imposition of a two-tier border control system.

Social implications – The paper is a catalyst for open debate on the fundamental questions of how we got to this point and where do we want to go. It questions the process by which the increased use of IT in border controls has become the norm and policy trend in Europe, and discusses where the limits could be drawn from a fundamental rights perspective. In particular, it warns against the institutionalisation of a two-tier border control system among third-country nationals.

Originality/value – Little attention is given to the fundamental rights concerns raised for EU and non-EU citizens as related to biometrics and their use in ABCs, and how these issues are reproduced in the Smart Borders proposal. The paper fills this gap by taking a bottom-up approach: examining the implications of individual elements of the proposal to see their impact on the broader policy.

Keywords Biometrics, Automated border control, EES, Fundamental rights, RTP, Smart Borders

Paper type Research paper

1. Introduction

Following a long period of transformation in Europe with regard to the conceptualisation of and legislation on border control, recent developments involve an increasing use of technological solutions, the main illustrations of which are the employment of databases (and their ever higher level of interconnectedness), biometrics, surveillance techniques and automatic border controls (ABC). Although they all represent separate issues with their own set of ethical and fundamental rights concerns, these different strands increasingly converge and are portrayed as sides of the same

The authors would like to acknowledge and thank the interview partners who took the time to speak with us, their input was invaluable. The research was conducted within the framework of a larger EU-funded project, "FastPass – A harmonized, modular reference system for all European automatic border crossing points", and the authors would like to thank the other partners of the project for their support.

Journal of Information, Communication and Ethics in Society
Vol. 13 No. 1, 2015
pp. 39-57

1477-996X
DOI 10.1108/JICES-02-2014-0008

coin, where one requires another to be implemented. This convergence in itself raises a series of ethical questions about the process by which this approach is becoming the norm and global trend. Furthermore, it can be paired with a general discussion on democracy and participation, touching upon issues of path dependency in decision-making, as well as the lack of vigorous debate among the broader public or even policymakers outside of the security-centred areas regarding the purpose, motives, main drivers and efficiency of advocated means to achieve the desired goals. Moreover, this approach reflects an implicit and unquestioned link between security concerns (threats) and immigration (foreigners)[1]. This poses the danger that the security approach is prioritised over fundamental rights concerns, without a debate on whether this is a desired approach or even efficient for any legitimate public policy purposes. The European Commission (EC)'s Smart Borders proposal represents a case in point of this trend. In its current form, it compounds all the separate issues mentioned above, and also raises additional questions of its own, particularly concerning its creation of a new divide among third-country nationals along questionable lines and criteria[2].

In this setting, the present paper examines the main concerns of biometrics and ABCs, as well as how they fit into the Smart Borders proposal. Distinguishing the fundamental rights perspective from the debates on ethics, the paper will primarily examine the role and implications of fundamental rights concerns in this process, asking questions about what brought us here and where do we want to go. At the same time it acknowledges, but does not address in detail, the broader questions about the use of biometrics in surveillance, nor does it dwell on the ethics of border control, which would encompass broader aspects related both to the legitimacy of control, as well as to its means and modes[3]. Furthermore, the paper will not enter into discussions regarding the actual feasibility of the proposal, of which there is already extensive research (Jeandesboz *et al.*, 2013; Hayes and Vermeulen, 2012).

First, the paper will look into the main issues at play regarding biometrics and their usage in ABCs, which are increasingly being implemented in Europe. Then it will focus on the Smart Borders proposal, which demonstrates the larger approach of facilitated freedom of movement for some and reinforced controls of others at the external borders of the European Union (EU), through an unquestioned integration of biometrics and ABC systems. The paper argues that the policy represents a trend of promotion of such technologies as a European-wide panacea for security, without considering the fundamental rights issues that are likely to arise. Moreover, similar to the divide created by the Schengen approach between travellers (EU vs non-EU), the use of new technologies in border control is buttressing new divides among third-country nationals ("high risk"-"low risk"), the implication being that rights are not the same for everyone. Such distinctions currently reflect a mix of arguments related both to immigration status and security concerns, enhancing the view that threats come from the outside and that foreigners (especially poor ones) are potential suspects, subject to additional controls.

2. Methodology

This article will present results from extensive background research and several qualitative in-depth interviews conducted in 2013 with key stakeholders[4]. The work has been supported by the FastPass project. The research leading to these results has received funding from the EU Seventh Framework Programme (FP7/2007-2013) under

grant agreement no. 312583. The nine interviews were conducted individually or with maximum two interview subjects in English, either in-person in private offices or via telephone. Interviews were chosen based on the interest and impact the stakeholder or their institution has on the development of ABCs and the implementation of the proposed EU Smart Borders initiative, with a particular view to include opinions outside of the security community. This included stakeholders from European institutions, non-governmental and inter-governmental organisations, academics and independent consultants as well as a representative of the industry to have a sample of the full spectrum of views on the topic. The interview results were complemented by extensive desk research to clarify the representativeness of the views expressed in interviews. Despite the limited number of interviews as well as the somewhat limited academic literature currently available on the topic and the rapidly changing field of research, the article demonstrates the wide spectrum of opinions on biometrics, ABC and the Smart Borders proposal, highlighting the key fundamental rights concerns as represented by certain stakeholders and in the literature.

Interviews were semi-structured, based on central interview guidelines that were developed by the authors and tailored for various stakeholder groups. This approach was selected to give subjects the liberty to discuss their opinions freely, to provide information outside the expectations and perceptions of the interviewer.

3. Fundamental rights framework

Based on past experiences with regard to biometrics and ABCs, and future scenarios highlighted in the Smart Borders proposal, in particular those highlighted by stakeholders interviewed, relevant fundamental rights issues at the European level will be highlighted.

Firstly, it should be noted that the Schengen Borders Code establishes the rules for conducting border checks at the border of the Schengen Area[5], and specifically highlights that fundamental rights should be ensured during the process, particularly those covered by the Charter of the Fundamental Rights of the European Union (European Union, 2000; Schengen Borders Code Council Regulation 562/2006 Recital 7, Recital 20). Although the Charter is the EU treaty highlighted by the Schengen Borders Code, the Council of Europe's (CoE) European Convention on Human Rights (ECHR) (Council of Europe, 2010) is closely connected, especially considering that all EU Member States are also members of the CoE. The ECHR allows that any person (including non-citizens) on CoE Member State territory who feels their rights under the ECHR have been violated, to take the case to the European Court of Human Rights (ECtHR). For this reason, relevant cases concerning border control at Schengen's external borders have also been taken to the ECtHR, in addition to national courts and the EU's European Court of Justice (CJEU). There is indeed an important body of ECtHR and CJEU case law clarifying and upholding the rights accorded during border checks, based on the rights accorded by EU law and the ECHR, including on the applicability of rights during detention in transit zones (*Amuur* v. *France*), guarantee of human dignity during border checks (*Mohamed Zakaria* CJEU case 23/12), access to effective remedy during accelerated returns (*Hirsi Jamaa et al.*, v. *Italy*) and application of detailed rules and minimum safeguards on measures that impact privacy (*S. And Marper* v. *UK*)[6]. Further, in 2014, the CJEU (*Digital Rights Ireland and Seitlinger and Others* Case C293/12) struck down the EU's Data Retention Directive (Directive 2006/24/EC) due to its

disproportional and not sufficiently restrictive interference on the rights of privacy and data protection.

As regards especially the use of databases and technology to record and verify identity, there are clear implications with regard to the right to privacy and data protection. According to European law (including: Charter Article 7, ECHR Article 8, Data Protection Directive, EC Regulation 45/2001 (2000), Treaty on the Functioning of the European Union Article 16), this right implies that a person's data must be processed only for a previously specified and legitimate purpose that is proportional to the aim, and with the consent of the person. Moreover, the process must be transparent to the person. This means not only the process by which the person's data are collected and verified, but also the means to rectify the data if incorrect. The latter overlaps with the right to effective remedy, also ensured by European law (Charter Article 47, ECHR Article 13).

The increasing recording of data as well as use of automation in border controls entails due attention to the right to effective remedy, for example: revision of incorrect data in a database or review of a denial of entry into the Schengen Area. Regarding the use of biometrics and new technology, this is especially important, as one should have the possibility not only to correct any inaccurate personal data but also to be able to remedy any misuse of data that has occurred. This includes not only misuse of data that may be due to forged identities (or biometrics), but also as regards decisions on visa and asylum matters if they are based on previously recorded information. In this latter case, the prior recording of biometric and biographic information in a database may impact future eligibility for a visa or for asylum, without the consideration that a person's situation can drastically change; where someone may not have been eligible for asylum previously, their situation may have so changed in the meantime that they are now eligible for protection.

Finally, as noted previously, all EU and Schengen Member States are also signatories to the ECHR. Therefore, these fundamental rights and others are applicable to all persons on the territory. Nonetheless, the validity and practical application of these protections at the border has at times proven problematic, due to the fact that border areas are often considered by states to be outside national jurisdiction (as the person has not yet entered the territory), and also the lack of or denial of presence of human rights non-governmental organisations[7]. The following sections will not focus on the fundamental rights implications of checks at the border in general, but rather will hone in on those rights relevant for the use of biometrics, ABCs and the Smart Borders proposal.

4. Biometrics and their usage in European ABC systems

4.1 Biometrics

Biometrics are currently considered by many in the security community as the most accurate means to determine a person's identity. Biometric data are characteristics or traits that can be used to identify a person, and can include fingerprints, facial recognition, DNA, iris recognition, retina, voice or even gait. However, in terms of data collected for immigration purposes and retained on an electronic chip within a passport or other travel document, this most commonly includes fingerprint, facial, iris and retina recognition. To choose one form of biometrics over another, a stakeholder involved in the International Standards Organisation Subcommittee on Biometrics (SC 37) noted

that the determination on which biometric data to use for processing travellers is not based solely on technical or feasibility issues, but also what is the global standard: "Here's all the ones on the planet and [. . .] you might see nobody's using vascular" (ST_1). Yet, when considering whether and which biometric data to use for border controls, ethical and fundamental rights concerns must also be considered at the same level.

When used for border control purposes, previously collected biometric data are compared with that given in-person upon arrival at the control. Advocates emphasise that its usage complements and enhances the security of traditional border controls, by "reinforcing" the verification of a traveller's true identity, and argue that such technology may improve privacy, by preventing identity theft and the usage of false identity documents (ST_2). According to the European Biometrics Group: "With the venue of the information society, identifying yourself with biometrics seems the safest way [sic] safest means to protect your identity against theft"(Feldman, 2012). Moreover, it is maintained that this could have a positive effect of increasing the difficulty with which traffickers and smugglers cross borders and use false identification documents (either for themselves or others). In this case, the argument further goes that travellers may become more confident in border controls, through the regular use of reliable and accurate data.

However, there are several privacy and data protection concerns that have been voiced regarding the collection and usage of such data on an individual, personal level, with a view to protection of fundamental rights. While technological developments can increase the reliability and security of biometric data, to date there are still issues with regard to errors (e.g. false-positives), vulnerabilities to interference (e.g. "skimming", or unauthorised reading of documents from a distance), forgery of biometric data[8] and production of biometric passports based on falsified breeder documents (e.g. birth certificates). In the latter case, breeder documents used to obtain a biometric passport have not greatly changed in the past decades, demonstrating that although a more secure machine-readable biometric passport has been created, it is still based on older, more easily forged, breeder documents.

These concerns particularly highlight that the use of biometrics does not necessarily mean increased security. As one interview noted: "Biometric passports are secured at the moment because they are super expensive to falsify them. Once the price of biometric passports will drop, then they will falsify that one, it's not a problem" (ST_3)[9]. This could present a new challenge in terms of identity theft, if biometric data could be forged and used, especially if these data are used for purposes of border control. These issues can be compounded if there are weak data protection regulations, unfamiliarity of travellers with the process and their rights and means to remedy and/or an expansion of the purpose or scope of usage of biometric data from what was originally foreseen. This latter concern is somewhat substantiated in the European case when one regards the increasing use and connectedness of European databases, where data are shared and used by previously unforeseen people and institutions, as will be noted later. The safeguard of rights to data protection and privacy can thus be compromised when security and border control are prioritised as the primary function for biometrics over human rights concerns, leading to sharing of biometric information beyond the original scope.

Additional concerns with biometrics involve hygienic and cultural reasons for not wanting to use such technology. With outbreaks of diseases (e.g. SARS), certain people may want to avoid using such scanning devices. Moreover, as biometrics involves collecting information that is intrinsically personal and private, its collection or the means of collection (directing a person's hands for a fingerprint, placing a person's face for iris scanning) itself may be objectionable to some cultures or religions for reasons of dignity (Vakalis *et al.*, 2006; Thomas, 2005).

This is also an issue for those who associate such collection methods with criminal activity or have a distrust of authority figures. There are widely differing attitudes to and "cultures" of privacy outside of and within Europe and as a result different degrees of acceptance of surveillance and other forms of collection of personal data, reflecting different historical experiences in the use and abuse of personal information by authorities[10]. Asylum seekers and others fleeing persecution may find such procedures extremely uncomfortable and frightening, and it may also trigger memories of state-directed persecution of own citizens based on comprehensive identification records in the authoritarian regimes in Europe's still recent history.

Although the use of biometrics has been argued to benefit the protection of asylum seekers, its usage continues to be a point of debate. On the one hand, registration through biometrics has been argued to enhance protection by allowing registration by those who may not have identity documentation and reducing the chances of fraud. On the other, asylum seekers have a clear stake in ensuring that their data remain confidential and secure, something that cannot be 100 per cent guaranteed, even if, for example, Europe's asylum database Eurodac may only transfer biometric data to third countries when authorised to do so by a Community agreement (Faraj, 2011). Moreover, linking biometrics to past asylum or visa applications may impact a future application; a person's situation may change dramatically for the better or the worse, and information given in past applications should not preclude a person's eligibility in the future (Faraj, 2011; ECRE, 2007). This may make it more difficult to reach safe and secure channels for asylum. In fact, the use of fingerprint biometrics has been linked to the practice of asylum seekers and irregular migrants destroying their own fingerprints to avoid identification (BBC News, 2004).

Finally, while costs may be reduced for European states through the use of biometric data, the costs actually may increase for individual travellers to have access to such technology (e.g. an electronic passport, travel to consulates for registration, etc.), while in certain countries, biometric documents may simply not be available, potentially raising the barriers to mobility (ST_2). In this case, promoting the usage of biometrics may lead to reinforcing an already existing divide between those countries with elaborate institutional structures, procedures and technologies, and those without, where coming from a country with poor institutionalisation will mean that individuals will automatically be treated as high-risk travellers and as such will be confronted with stronger controls and higher barriers to mobility.

Thus, although biometrics have been hailed as a secure means to verify identity, it is clear that there are still many shortcomings that need to be addressed. Namely, that there are several ways in which the use of biometrics in travel documents is not secure (e.g. breeder documents, skimming), and that there remain serious fundamental rights concerns with regard to their usage (e.g. privacy, non-refoulement).

4.2 ABCs in Europe

Increasingly in Europe, biometric data are being used in conjunction with ABC. As of 2013, 14 EU or Schengen countries had ABC systems in operation or piloting phase, in some cases already combined with registered traveller-like systems (Commission Staff Working Paper SWD, 2013). These systems have been identified as useful for the same purpose of "reinforcing" the security of verification of a traveller's identity, in addition to a reported increased efficiency and speed in conducting border control:

> Passenger numbers are going up [. . .] but the numbers of officers that we can afford to deal with those passengers is staying the same or going down [. . .] Therefore we have to look for new methods to deal with it [. . .] What can we do to deal with a decision which is very, so to speak, black and white, yes or no, are you or are you not EU citizen [. . .] a machine could do it. (ST_4, Also ST_8)

In this regard, ABC systems are considered by European border agencies and border guards as a useful filter, allowing low-risk (currently primarily European) travellers to enter with a minimal identity check and retaining border guards to focus on other priorities, including checks on higher-risk (currently primarily non-European) travellers. Indeed, policymakers across the board point out that border guard work at ABC gates should be a complement to, rather than a replacement of, manual controls by border guards (Frontex, 2007 and ST_8). It is instead the potential for obtaining standardised, comparable and reliable results of identity checks, which seems to be a driving force in establishing ABC (ST_8).

ABC systems are principally of two types:

(1) one where the system accesses and verifies the biometric data on an electronic chip in the travel document against that obtained through the various scanning systems within the ABC system; and

(2) the second does the same verification, but against a database to which the person has previously registered, rather than against the information in the travel document.

In the former case, the registration of the biometric data and issuing of documents is done by various national institutions, while in the latter, a sufficient infrastructure and centralised database is needed to collect and store the data of the registered traveller in a systematic way. In Europe at present, ABCs are mostly of the first type and primarily process EU/European Economic Area (EEA)/Schengen citizens with e-passports. In this case, national institutions collect biometrics to store in the e-passport, and should delete them from their own databases (according to national law). However, the potential Smart Borders initiative would likely require the wider implementation of the second type of system, to process third-country nationals enrolled in a European Registered Traveller Programme (RTP)[11]. In this case, a more strongly developed European infrastructure is required both to collect and store biometrics of those registered travellers (for the RTP), as well as to document and store the biometric and biographic information of all third-country nationals entering and exiting the Schengen Area (for the EES), as will be discussed in the next section.

The use of biometrics in border controls generally and ABC systems specifically has been discussed by European stakeholders for its potential to limit ethnic profiling and ensure non-discrimination through automated processing of travellers:

> If you automate it you take out the human evaluation element of the border guards, which also can be used in the wrong sense as well. You know, to identify someone as a potential suspect or something just based on physical appearance. An automated system could potentially correct that, but at the same time it doesn't allow for any sensitivity. (ST_7, Also ST_3, ST_4, ST_9)

In this case, there is the concern that humans may base their decisions based on race, ethnicity or gender rather than other indicators such as port of departure or nervousness. Although ethnicity does at time play a role in a decision, there is the concern that a human may base his or her decision solely on this, rather than taking other factors into account. Thus, through the use of ABC, the decision becomes an automatic one, where if the biometric data given in-person match that within the travel document, the person should be allowed entrance, no matter his or her background, thus ensuring against potential discrimination by a human border guard. Nevertheless, there have also been arguments that ABC gates could be programmed to use discriminatory algorithms that could, for example, be programmed to stop all persons of a certain nationality, or those arriving on certain high-risk flights. This kind of profiling translated to algorithm may walk a thin line between risk-based profiling and ethnic profiling.

According to the Frontex (2010) studies on the functioning of ABC systems, their key requirements involve a combination of security and practical concerns, but also a consideration for fundamental rights, particularly data protection and privacy, as access to the information provided by such ABC systems and linked databases is to be strictly regulated to ensure against misuse. The EU Agency for Fundamental Rights also highlighted these issues in its recommendations on usage of ABC gates, relevant for all, as even EU citizens are subject to non-systematic database queries:

> When querying border control records stored in databases, due diligence by the responsible administration needs to be respected and privacy by design reflected in the development of the systems. There are also concerns regarding the identification of victims of trafficking, the protection of the rights of the child, the rights of persons with disabilities, and those of elderly persons (FRA, 2013).

These questions were particularly highlighted by both interviews with European political stakeholders as issues that should be discussed at a European level and the approaches to which should be harmonised (ST_8, ST_9). Indeed, ABC systems are currently lacking in terms of identification of groups at risk, especially potential victims of trafficking, as emphasised by one interview: "For victims of THB [trafficking in human beings], indication of purpose is quite difficult. Now with automatic border controls then you give advantage to organisers, absolutely" (ST_3). Usage of the systems by minors in particular can be problematic due to the difficulty in assessing the relationship between a minor and his or her adult companion. Moreover, for those with disabilities and the elderly, ABC systems are not uniformly adapted to process these groups (e.g. for reasons of height restrictions or narrowness of the e-gates in the case of the former, and visibility of instructions and delayed reaction time in the case of the latter). These issues bring up the "duty of care" that border guards have, where discretionary power that can be used by humans to, for example, ask follow-up questions to a potential victim of trafficking or an unaccompanied minor is no longer available. Border guards have repeatedly highlighted the role of human intelligence and

discretion in border checks, and a recent Frontex study confirms that humans are better than machines at dealing with exceptions such as these (Frontex, 2014). When this important role of the human and human intelligence is transferred to automated systems that use data and algorithms, there are likely to be negative impacts on the assurance of fundamental rights, particularly of vulnerable groups.

This ongoing debate over biometrics and their use in ABC systems shows how new technologies are foreseen to greatly improve security and facilitate movement, but still have some clear fundamental rights issues that should not be de-prioritised along the way. As one stakeholder noted, in today's world one could:

> [. . .] build our DNA in passports and you would have tamper-proof 100 per cent [. . .] [But] what is secured enough? Because 100 per cent security will come at a certain cost of other social and ethical issues (ST_2).

In the push to have secure verification of identity and secure borders, one must still consider the consequences of their usage for various groups and society at large. No technology is perfect, thus it is important to examine the impact of such technology on the broader environment of border control policies, linking the technology with the policy implications.

5. The Smart Borders proposal

Examining the concerns with regard to the usage of biometrics and ABC in Europe provides important lessons for European border management policies, especially as biometrics, databases and ABC systems become increasingly relevant and inter-related for these policies. The linkage between policy on freedom of movement within the EU and control of the external borders has been, from the outset, considered as two sides of the same coin, where one side is needed for the other to succeed:

> Free movement as introduced within the territory of the Schengen States [. . .] is a freedom which as a counterpart requires the strengthening of the external borders of that area and a policy for the removal of illegally resident aliens which is effective and dissuasive [. . .] It is indeed this double axiom which guides EU action in this sphere (Council of the European Union General Secretariat, 2002).

Although this dichotomy began with the freedom of movement of European citizens within the EU/Schengen Area and increased controls of third-country nationals entering the Area, it has now developed into a more sophisticated system, where biometrics, ABC and databases play an important role.

Over the years, various European databases storing information collected at Member State level have been developed for use in border controls across the EU's external borders, especially related to asylum applicants and irregular migrants (European Dactyloscopy, or Eurodac, biometrics collected), criminals (Schengen Information System I and II, or SIS, biometric collection possible) and those applying for a EU visa (Visa Information System, or VIS, biometrics collected). In 2013, two new databases – EES and RTP – were proposed. They closely mirror the two-pronged approach of increased controls for some on the one hand, and facilitation of movement of others on the other: the EES records entries and exits to and from the EU of third-country nationals admitted for short stays, and the RTP allows registered third-country national travellers to use ABCs. Both include biometric identification by fingerprints, maintaining the same technical requirements as the other databases.

All of the above EU databases are to be managed centrally by the EU Agency for large-scale IT systems (eu-LISA). Established in 2012, this agency is tasked with maintaining the functioning of these systems and in particular "ensuring the continuous, uninterrupted exchange of data between national authorities" (European Commission, 2014). It should also maintain the separation of data in the various systems, to ensure security and data protection requirements.

While some see database use as a precondition for efficient border controls, for others the increasing interoperability and coordination between databases across EU Member States signals a future where such data could be used as a form of surveillance (ST_5, ST_6): "The more this data is transferred across different agencies and countries, the greater the risk of it seeping into controversial areas of immigration control, such as tracking and surveillance" (Thomas, 2005). Moreover, once a system is created, additional uses can be found for it, not necessarily ending with border control (Vakalis *et al.*, 2006). This can especially be observed with the re-vamped version of Eurodac; originally created to collect and compare fingerprints of asylum seekers, irregular border crossers and those illegally present within EU territory, the forthcoming amendment will allow national police forces and Europol to compare fingerprints linked to criminal investigations with those in Eurodac (European Commission, 2013). The protection of rights to data protection and privacy can thus be compromised when security and border control are prioritised as the primary function for biometrics over fundamental rights concerns. This becomes even more problematic when applied only on the basis of legal status or nationality, whereas all persons should have access to and protection of the same fundamental rights.

At the moment, the Smart Borders initiative is only in proposal form, and even according to the Commission: "there is no single person who can say at the moment what will exactly be the end result", including with regard to access restrictions and use of biometrics (ST_8). Nonetheless, according to the Commission, the proposal reflects a balanced approach:

> Security, facilitation and data protection and fundamental rights they had an equal footing, meaning that at some stage some things which are proposed by the Commission might not be operationally perfect, but on the other hand this is not the only thing that needs to be considered [. . .] (ST_8).

Yet, the necessity, proportionality and feasibility of establishing an EES and RTP have already become points of controversy in inter-institutional debates, and the package has been criticised by some Member States, the European Parliament, the European Data Protection Supervisor (EDPS) and the Commission's own Impact Assessment Board, particularly in the absence of an evaluation of the functioning of SIS II and VIS.

None of the European databases functioning to date record entries and exits of third-country nationals to and from the Schengen Area; however, this was identified as a key area for development; as early as 2004, an impact assessment of VIS examined the establishment of an entry-exit system as one of the possible policy options (EPEC, 2004). Currently, 14 EU/Schengen States operate entry/exit-like schemes (Jeandesboz *et al.*, 2013), yet at present, the data collected nationally are not shared with other states. Thus the reasoning for an EU-wide database, which is tasked with: "improving the management of the external borders and the fight against irregular immigration" (Commission Proposal COM, 2013b 95 final). The proposed system would provide an

EU-wide record of entries and exits of all third-country nationals travelling for a short stay (90 days within 180 days) to and from the Schengen Area, including those not currently requiring a visa for short-term stays. Such a system would allow for more reliable data on several fronts: whether those entering the Area typically exit through the same state as that to which he or she arrived, the extent of travel to and from the EU and, significantly, the number of overstayers[12] irregularly present within the EU. A Commission interviewee confirmed: "This will also help the police guys working within the territory so that overstayers at least be identified if they are found in the territory" (ST_8). This is a key point of the proposal, as the EES is foreseen as a tool for the EU to obtain reliable data on irregular migrants present in the EU, and would play a part in assessing a person's future eligibility for travel to the EU, based on whether he or she has been identified as an overstayer in the past. However, one stakeholder noted that, while unlikely, information on overstayers could bring benefits in terms of fundamental rights protection:

> Depending on how this would be implemented with the Member States maybe something could be done for them to be able to access their fundamental rights as well. It really depends on how you use the technology you have and for which purpose. (ST_7)

Chief among the concerns with the EES is the fact that the system itself cannot identify suspected terrorists or perpetrators of serious crime, but can only provide information as to whether the suspect has left the Schengen Area legally (Peers, 2008). In conjunction, an EES cannot locate overstayers within the EU, although it could have a deterrent effect on potential overstayers. Some stakeholders believe that this could lead to discriminatory surveillance practices within the EU to detect such overstayers (ST_5, ST_6):

> The merits of doing it are sort of dubious, if you are only catching the so-called overstayers on the way out when they've already overstayed and they were going home anyway. The other alternative is to link it to the much more sort of draconian policing system, and in that case, there probably is a good chance that it will feed into practices like discriminatory stop and search on the streets [. . .] (ST_5).

To avoid being identified as an overstayer, such a system could have a contradictory effect of increasing the rate of illegal entry; increased illegal entry could also potentially expand the usage of smuggling and trafficking networks, which have their own harmful implications in terms of fundamental rights concerns.

Considering there is no clear current European policy on the management of overstayers, the creation of an additional large-scale database to store massive amounts of data can be considered a disproportionate response to a problem that may be better addressed in other ways. Indeed, considering the sheer amount of data collection proposed for an EES, this presents a clear issue with regard to proportionality. The European Data Protection Supervisor (2013) and others (Hayes and Vermeulen, 2012) have argued convincingly that the EC has failed to demonstrate that the amount of data collected is proportional to the goal of reducing irregular immigration. Furthermore, given that the routine functioning of the system will imply a need to exchange personal information with third countries in relation to the return or removal of individuals, data protection rights of these individuals should also be ensured, to avoid placing the person in danger (EDPS, 2013).

The voluntary RTP has as its key object "to facilitate the crossing of the European Union external borders by frequent, pre-vetted third-country travellers", an estimated 0.2 per cent of total passenger flows (Commission Proposal COM, 2013b 97 final). It is expected to reduce the time and cost of border crossing for those enrolled in the programme, as well as improve movement through border crossing points. In 2008, the RTP was already considered as a complementary system to the EES, through: "[. . .] speeding up border crossing times and (probably) offsetting the costs of the entry-exit system" (Peers, 2008). So from early on, the two measures were considered intrinsically linked, as the additional burden on border control of the EES is considered to be offset by an RTP where members would be offered a simplified and automated entry process, as they would have gone through an extensive pre-screening process:

> When we start capturing for example fingerprints [during exit controls] it causes some delays, but that's why we really see that we need to have a registered traveller program to balance all these things. That's the thing that also needs to be checked with the automation [. . .] so that [the ABC system] can interrogate in the registered traveller program and it can interrogate with the entry-exit system and all this is done automatically. (ST_8)

As noted above, ABC systems are considered a main component for the programme to function properly, and are specifically cited throughout the proposal for their proven efficiency to date in biometric processing of EU citizens, which should now be extended to certain third-country nationals. The system would require pre-registration of third-country nationals according to set and standardised criteria (e.g. sufficient means, journeys purpose). Once approved, the person would be provided with a machine-readable token for use in an ABC system, where the biometric information given in person would be compared against those in the RTP database. Minors above the age of 12 would also be allowed to register for the RTP, provided that permission is given from their parent or guardian. Nonetheless, the Commission interviewee highlighted that steps should still be taken to ensure that minors are protected from potential abuse of the system, although there was no elaboration on what this might entail (ST_8). These basic criteria are then supplemented by an assessment of the applicant's reliability, explicitly noting that:

> [. . .] particular consideration shall be given to assessing whether the applicant presents a risk of illegal immigration or a risk to the security of the Member States and whether the applicant intends to leave the territory of the Member States within the authorised stay (Commission Proposal COM, 2013b 97 final).

Thus, the RTP is linked with prevention of irregular immigration at large, and therefore also the EES, as a proposed system to identify such irregular immigrants as overstayers.

The main critiques regarding the RTP involve not only its feasibility, as many similar programmes have had problems with implementation and limited use, but also a larger concern related to access. The RTP has been criticised for creating a new distinction among travellers, between "undesirable/high risk" and "desirable/low risk" candidates:

> [The RTP], under which business and other frequent travellers would benefit from faster crossings, will institutionalise a two-tier border control system in the EU based on crude indicators such as wealth, nationality, employer and travel history (Bigo *et al.*, 2012).

Limiting the group eligible for the RTP to such an elite class of persons has implications not only for the actual feasibility of the programme (considering the limitations), but also importantly in terms of non-discrimination in setting the criteria by which individuals are assessed.

Regarding the initiative as a whole, it has been critiqued based not only on the feasibility of similar large-scale initiatives that experienced major difficulties in development, deployment or functioning[13], but also in its own right. In particular, the same fundamental rights concerns with regard to use of biometrics arise again as their collection within new large-scale databases are a critical characteristic of the initiative. Moreover, there are serious concerns regarding the right to legal remedy; in the context of automated border procedures and a multiplication of databases, exercising this right when an unfavourable decision is taken becomes increasingly difficult (EDPS, 2013). For many, the initiative reflects a pattern of path dependence rather than an actual need for further measures involving large-scale IT systems in EU border control policies, at the expense of impartially assessing the need and impact beforehand (Ibid; Jeandesboz *et al.*, 2013):

> What is likely to happen is: set the system up first and then give law enforcement access afterwards [. . .] I think it would be very simple to say, look, if this is indeed an immigration control measure, then the only people who need to have access to this are the immigration services. If it is a counter-terrorism or security or policing measure well then let's have a debate about that during the legislative process. Sadly, I don't think that's going to happen. (ST_5)

A move towards creating one of the world's largest biometric databases to track and identify overstayers, with a view of eventually extending access to law enforcement, has troubling implications about the amount of surveillance and tracking that could be applied in the future within the EU. Already applied to third-country nationals, some believe this could be expanded:

> In envisaging the gradual replacement of border guards with "Automated Border Control" gates, the planned "smart borders" proposals may also pave the way for increased surveillance of EU citizens, whose movements could easily be recorded and stored in future (Bigo *et al.*, 2012).

The recent Snowden revelations have brought to the surface questions regarding surveillance of own citizens and how information is collected and used, as well as the possibility that classified information may be broadcasted and shared through "leaks". They have shown in practice the concerns highlighted above: set up a data collection system first, then expand its access and field of collection afterwards. Although it is clear that systems at the moment should be clearly separated and access limited, there are already indications of plans for future access of law enforcement: Eurodac's forecast regulation has already shown such an expansion, and the EES has already been identified as an effective tool for law enforcement (Council of the European Union, 2013).

Automation of these controls also implies a progressive transfer of power and discretion on the control and uses of the data (collected by classical national authorities and individual border guards) to various EU levels and actors, without a larger discussion on the implications of such a transfer (Carrera *et al.*, 2013).

While there are certain advantages to the implementation of a European EES and RTP, there are still many valid concerns, related both to the systems themselves as

well as to the connected concerns with regard to usage of biometrics and ABC systems, all clearly dependent on the rules set up at the start on the scope and purpose of the system. One can recognise in its clear goals of identification of overstayers on the one hand and facilitation of selected travellers on the other, the dichotomous approach Europe is taking in border management: facilitation of a selected group, at the expense of another. The Smart Borders initiative, which deeply integrates biometrics and ABCs into its approach without question, facilitates the movement of certain pre-vetted travellers within, into and out of the EU, while implementing increased security measures for "higher risk" travellers, essentially generating and reinforcing social divides.

6. Conclusions

By examining the main concerns regarding biometrics and ABCs, and how they relate to the recent Smart Borders initiative, one can observe how new technologies are developing in conjunction with each other, each overlapping and building upon the last but without a serious consideration of the wider fundamental rights implications. The emerging European vision of e-borders has grown from broader trends in Europe and world-wide, where technology is increasingly viewed as an essential tool for the control of external borders. At the same time, debate on the use of such new technologies for border control highlights challenges for development and use of such systems. Serious concerns still remain regarding privacy and data protection, ranging from the most basic questions regarding biometrics and their usage within larger automated systems for border control, to the broader policies being proposed, with each level integrating such data and systems implicitly, without questioning the consequences on their current and future functioning. So deeply integrated in the Smart Borders proposal, biometrics and ABC systems are apparently considered essential tools in enhancing European border controls. Yet they are not a panacea and should not be considered as such, particularly when one examines the considerable fundamental rights concerns and the clear limits in this regard by European legislation. In this context, a reconsideration of the necessity and proportionality of the Smart Borders proposal becomes essential.

Moreover, while technology can of course be useful for a variety of purposes, in the context of border controls it appears to be increasingly used as a tool to distinguish or bolster the rights accorded to a certain group of persons in contrast to another group, subject to increased controls. Biometrics and ABC systems already represent in practice tools to enhance security at borders: in the former case, with the objective of improving identification while decreasing the possibility for fraud, and in the latter, by using biometrics to facilitate movement of EU/Schengen citizens. Although initially differentiating primarily between EU citizens and third-country nationals, recent developments reflect a changing mindset in Europe, where freedom of movement is gradually being considered relevant for certain third-country nationals within particular contexts, with an important role for biometrics, databases and ABC systems. Now, with the Smart Borders proposal, a new line would be drawn: not only between EU/Schengen and third-country nationals, but even further among the latter, where the movement of those with easier access to biometric passports and already pre-assessed to be "low risk" would be facilitated through automated controls, while more attention would be paid to "more risky" third-country nationals. This compounds the

fundamental rights issues already highlighted, as such a division implies that the rights accorded to some are not available to everyone. Enforcing a scenario where third-country nationals must prove their innocence, by submitting biometric and other personal data, European policy walks a very thin line between security and fundamental rights. While security concerns are clearly at the fore in border control policies, they cannot overshadow the rights every individual must be accorded while crossing a border.

Notes

1. For more on migration as a security issue, see Huysmans (2006), Huysmans and Squire (2009) and Benam (2011), and as a criminal offence, see Bigo (2004) and Anderson (2013).
2. Risk criteria are set out in Article 21 of the Visa Code (see Council Regulation 810/2009). This term, however, is quite elusive and vague, and not legal terminology.
3. For more on these aspects, see Pécoud and de Guchteneire (2006) and Palm (2013, 2011).
4. In selecting interviewees, we targeted individuals deeply involved in debates on border control. In addition, interlocutors typically are likely to express institutional views, limiting the scope for additional information that could be obtained through additional interviews with members from the same group. Outside of public institutions, social, legal and political expertise on issues of biometrics in border control and smart borders at large is limited to small circle of experts, while developers, both from industry and from academic institutions, typically have a limited insight into fundamental rights or policy aspects of border control.
5. The Schengen Area is an area of free movement established across 26 states (primarily European Union Member States, but also including some Schengen-associated countries). Border controls have been eliminated between these 26 countries, but exist at the "external borders", i.e. where a person may enter the country from a non-Schengen country.
6. For an overview of European law (EU, CoE) related to borders, see FRA (2014).
7. For more information on this, see Doctors Without Borders (2010) for their report on Italy's migrant centres, as well as the ECtHR case *Amuur v. France*, on applying protection to those held in international zones in airports. See also FRA (2015) for more information on fundamental rights concerns at European airports.
8. See, e.g., the reports from Hong Kong on successful attempts to pass through their ABC system using fake fingerprints (Hong Kong Legislative Council, 2012).
9. For a more comprehensive look at the ethical concerns related to biometric passports, see Palm (2013).
10. In Germany, fierce debates about privacy issues not only massively delayed the last traditional census taken in Germany (initially planned for 1981, finally conducted in 1987), but also made it impossible to conduct a traditional census since. An important byproduct of the controversy was the "census judgement" of the Constitutional Court in 1983, in which the principle of "informational self-determination" (*Informationelle Selbstbestimmung*) was laid down, the corner stone of current privacy legislation in Germany (Der Sächsiche Datenschutzbeauftragte, 2008).
11. Or a mixture of the two, as can be seen in Portugal. In Portugal, some of the ABC gates are programmed to also process pre-registered Angolan citizens.

12. "Overstayers" refers to persons who enter the EU legally but remain beyond the time limits of their stay. This is considered a key challenge in the EU, as estimates of undocumented migration in Europe found that the overstayers represent a key proportion of irregular migrants in the EU (Clandestino Database on Irregular Migration, 2012).

13. See, for example, GAO (2010) and House of Commons Home Affairs Committee (2012).

References

Anderson, B. (2013), *Us and Them? The Dangerous Politics of Immigration Control*, Oxford University Press, Oxford.

BBC News (2004), "Sweden refugees mutilate fingers", available at: http://news.bbc.co.uk/2/hi/europe/3593895.stm (accessed 9 September 2014).

Benam, C. (2011), "Emergence of a 'Big Brother' in Europe: border control and securitization of migration", *Insight Turkey*, Vol. 13 No. 3.

Bigo, D. (2004), "Criminalization of 'migrants': the side-effect of the will to control the frontiers and the sovereign illusion", Bogusz, B., Cholewinski, R., Cygan, A. and Szyszczak, E. (Eds), *Irregular Migration and Human Rights*, Martinus Nijhoff Publishers, Leiden.

Bigo, D., Carrera, S., Hayes, B., Hernanz, N. and Jeandesboz, J. (2012), *Justice and Home Affairs Databases and a Smart Borders System at EU External Borders: An Evaluation of Current and Forthcoming Proposals*, CEPS, Brussels.

Carrera, S., Hernanz, N. and Parkin, J. (2013), *Local and Regional Authorities and the EU's External Borders, A Multi-Level Governance Assessment of Schengen Governance and 'Smart Borders'*, European Union, Brussels.

Clandestino Database on Irregular Migration (2012), available at: http://irregular-migration.net/ (accessed 2 February 2014).

Commission Proposal COM (2013b), *97 Final of 28 February 2013 on a Regulation of the European Parliament and of the Council Establishing a Registered Traveller Programme*, Commission Proposal COM, Brussels.

Commission Staff Working Paper SWD (2013), *50 Final of 28 February 2013 Impact Assessment Accompanying Document to the Proposal for a Regulation of the European Parliament and of the Council Establishing a Registered Traveller Programme*, Commission Staff Working Paper SWD, Brussels.

Council of Europe 4.XI. 1950 of 1 June (2010), *Convention for the Protection of Human Rights and Fundamental Freedoms*.

Council of the European Union (2013), "Access for law enforcement purposes: summary of the replies to the questionnaire", 13680/13, Brussels, 10 October.

Council of the European Union General Secretariat (2002), *EU Schengen Catalogue: External Borders Control, Removal and Readmission: Recommendations and Best Practices*, Council of the European Union, Brussels.

Council Regulation 45/2001 of 18 December 2000 on the Protection of Individuals With Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data, Council Regulation, Brussels.

Council Regulation 562/2006 of 15 March 2006 establishing a Community Code on the Rules Governing the Movement of Persons Across Borders (Schengen Borders Code), Council Regulation, Brussels.

Council Regulation 810/2009 of 13 July 2009 Establishing a Community Code on Visas (Visa Code), Council Regulation, Brussels.

Der Sächsiche Datenschutzbeauftragte (2008), "25 Jahre Volkszählungsurteil", available at: www.saechsdsb.de/ueberblick-alle-themen/350-25-jahre-volkszaehlungsurteil (accessed 2 February 2014).

Doctors Without Borders (2010), "On the other side of the wall: a tour of Italy's migrant centres", available at: www.doctorswithoutborders.org/sites/usa/files/MSF-On-the-Other-Side-of-the-Wall-report-summary.pdf (accessed 11 September 2014).

ECRE (2007), *Defending Refugees' Access to Protection in Europe*, ECRE, Brussels.

EDPS (2013), *Opinion of the European Data Protection Supervisor on the Proposals for a Regulation Establishing an Entry/Exit System (EES) and a Regulation Establishing a Registered Traveller Programme (RTP)*, EDPS, Brussels, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-07-18_Smart_borders_EN.pdf (accessed 2 February 2014).

EPEC, European Policy Evaluation Consortium (2004), *Study for the Extended Impact Assessment of the Visa Information System. Final Report*, EPEC, Brussels, available at: www.statewatch.org/news/2005/jan/vis-com-835-study.pdf (accessed 2 February 2014).

European Commission (2013), "Identification of applicants (EURODOC)", available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/asylum/identification-of-applicants/index_en.htm (accessed 2 February 2014).

European Commission (2014), "EU Agency for large-scale IT systems", available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/agency/ (accessed 2 February 2014).

European Data Protection Supervisor, E.D.P.S. (2014), "Data protection", available at: https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection (accessed 2 February 2014).

European Union 2000/C 364/01 of 7 December (2000), *Charter of Fundamental Rights of the European Union*, European Union, Brussels.

Faraj, A. (2011), "Refugees and the biometric future: the impact of biometrics on refugees and asylum seekers", *Columbia Human Rights Law Review*, Vol. 42, p. 891.

Feldman, G. (2012), *The Migration Apparatus: Security, Labor, and Policymaking in the European Union*, Stanford University Press, Stanford.

FRA (2013), *Fundamental Rights: Challenges and Achievements in 2012, Annual Report 2012*, Publications Office of the European Union, Luxembourg.

FRA (2014), *Handbook on European Data Protection Law*, Publications Office of the European Union, Luxembourg.

FRA, European Union Agency for Fundamental Rights (2015), *Fundamental Rights at Airports: A Report on Border Checks at Five Airports in the European Union*, Publications Office of the European Union, Luxembourg.

Frontex (2007), *BIOPASS: Study on Automated Biometric Border Crossing Systems for Registered Passengers at Four European Airports*, Frontex, Warsaw.

Frontex (2010), *BIOPASS II: Automated Biometric Border Crossing Systems Based on Electronic Passports and Facial Recognition: RAPID and SmartGate*, Frontex, Warsaw.

Frontex (2014), "Document challenge II: deep dive seminar", *Secure Document World*, London, 18 June.

GAO (2010), "US-VISIT pilot evaluations offer limited understanding of exit options", Report to Congressional Committees, available at: www.gao.gov/assets/310/308630.pdf (accessed 2 February 2014).

Hayes, B. and Vermeulen, M. (2012), *Borderline: The EU's New Border Surveillance Initiatives*, Heinrich Böll Foundation, Berlin.

Hong Kong Legislative Council (2012), *Report of the Panel on Security for Submission to the Legislative Council*, CB2/PL/SE, Hong Kong.

House of Commons Home Affairs Committee (2012), *Work of the UK Border Agency (August-December 2011)*, The Stationery Office Limited, London.

Huysmans, J. (2006), *The Politics of Insecurity: Fear, Migration and Asylum in the EU*, Routledge, London.

Huysmans, J. and Squire, V. (2009), "Migration and Security", Balzacq, T. and Cavelty, M.D. (Eds), *Handbook of Security Studies*, Routledge, London.

Jeandesboz, J., Bigo, D., Hayes, B. and Simon, S. (2013), *The Commission's Legislative Proposals on Smart Borders: Their Feasibility and Costs*, European Parliament, Brussels.

Palm, E. (2011), *Towards an Ethically Defensible Migration Management – The Case of Surveillance-Based Migration Control*, AFSP Congrès, Strasbourg.

Palm, E. (2013), "Mobility and personal identity – rights and interests at stake in the development of EU's novel e-passport", *10th Annual IMISCOE Conference*, Malmö, 26-27 August.

Pécoud, A. and de Guchteneire, P. (2006), "International migration, border controls and human rights: assessing the relevance of a right to mobility", *Journal of Borderlands Studies*, Vol. 21 No. 1, pp. 69-86.

Peers, S. (2008), "Proposed New EU Border Control Systems", Briefing Paper, European Parliament, Brussels.

Thomas, R. (2005), "Biometrics, international migrants and human rights", *Global Commission on International Migration*, Geneva, January.

Vakalis, I., Hosgood, B. and Chawdhry, P. (2006), *Biometrics for Border Security – An Overview*, European Communities, Luxembourg.

Further reading

Commission Proposal COM (2012), *11 Final of 25 January 2012 on 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)*, Commission Proposal COM, Brussels.

Commission Proposal COM (2013a), *95 Final of 28 February 2013 on a Regulation of the European Parliament and of the Council Establishing an Entry/Exit System (EES) to Register Entry and Exit Data of Third Country Nationals Crossing the External Borders of the Member States of the European Union*, Commission Proposal COM, Brussels.

European Parliament and Council Directive 95/46/EC 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, European Parliament and Council Directive.

ICAO (2004), *Biometrics Deployment of Machine Readable Travel Documents Technical Report*, ICAO, Montréal.

About the authors

Maegan Hendow is currently a Researcher with ICMPD, focusing on fundamental rights issues related to border controls and border management. She has a BA degree from the University of California, Santa Barbara, including a year of study at the Institut d'Etudes Politiques of Lyon, and a joint master's degree in global studies from the University of Leipzig and the University of

Vienna. Maegan Hendow is the corresponding author and can be contacted at: maegan.hendow@icmpd.org

Alina Cibea has been part of the migration research unit at ICMPD for the past five years. She holds an MA degree in international studies from the Diplomatic Academy of Vienna and a BA degree in political science from University of Bucharest. Research interests include fundamental rights and anti-discrimination, the politics of border controls and processes of migration policymaking.

Albert Kraler has a degree in political science and African studies. Currently the Programme Manager of ICMPD's research programme, he has worked and studied at the University of Sussex, the School of Oriental and African Studies in London and the University of Vienna, currently serving as an Associate Lecturer at the University of Vienna.