Biometrics Please! Automated Border Controls & Data Protection Obligations

***Diana Dimitrova**, a legal researcher at ICRI, KU Leuven, focuses on privacy, data protection, and border control in the framework of the FastPass project. In this post she argues that the automation of border control in the EU increases the data protection obligations of the respective authorities and necessitates legislative changes.*

Most Member States of the EU are members of the Schengen Area. In other words, they must carry out border checks in accordance with the Schengen Borders Code (SBC). The check includes, *inter alia,* the presentation of a travel document and establishment of link between the travel document and the passenger (i.e. identity verification). The nature of this verification, however, changes when the process is automated.

Recently, border control has become increasingly automated. For example, when flying in and out of the Schengen Area, but also in and out of the UK, there are e-Gates for Automated Border Control (ABC). Although ABC is implemented differently across the EU, e-Gates usually allow passengers to scan their passports and to present their face, fingerprints or even iris for identity verification. These are called biometric identifiers.

Processing sensitive personal data at borders

ABC results in the automated processing of (biometric) data and thus brings along more responsibilities to the respective authorities as controllers of passenger data.

Biometrics constitute personal data and tend to be treated as sensitive due to the unique information they contain (see S and Marper vs UK judgment and Article 29 Working Party). Their processing in the border control context raises certain privacy and data protection issues, which have not been sufficiently debated.

The *Schwarz* judgment by the Court of Justice of the European Union (CJEU) ruled that including fingerprints in the chip of the biometric passports of EU citizens pursues the legitimate aim of preventing illegal entry into the EU. In his opinion, Advocate General Mengozzi however argued that fingerprint *verification* of EU citizens at the external borders of the EU is supposed to be done only non-systematically, i.e. only when doubts exist as to whether the passport belongs to the passenger presenting it.

Biometrics automate the identity check

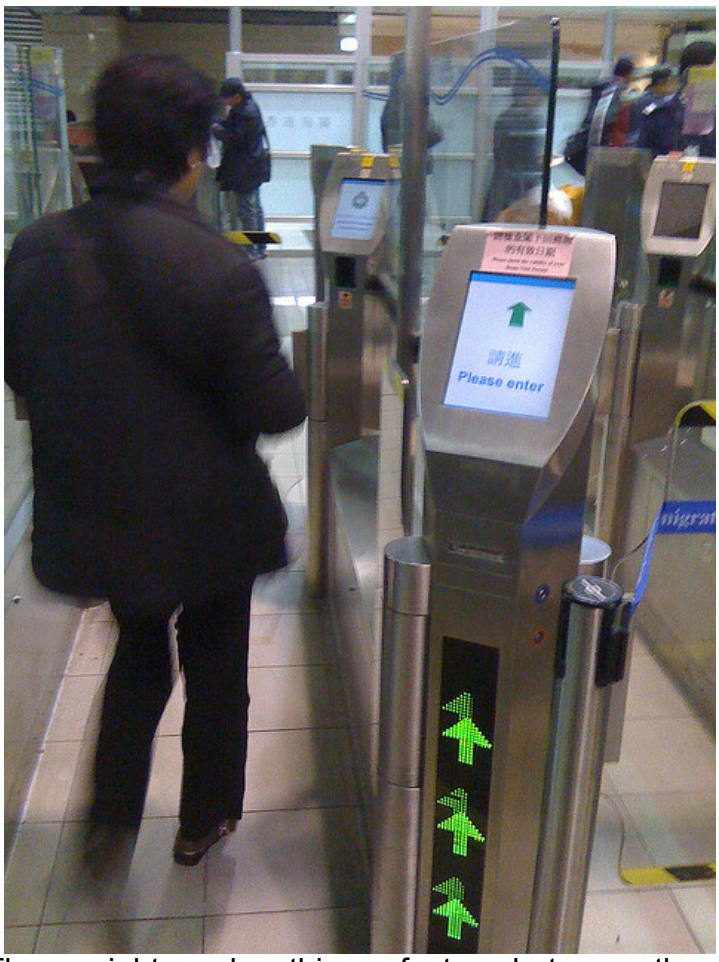
Whereas in manual border control the border guard visually compares the picture with the passenger, in ABC this verification is automated. As explained above, most EU e-passports contain a chip with 2 fingerprints and/or facial image. At e-Gates a live scan of the biometric identifier(s) is taken and compared to the biometric(s) on the passport chip. Alternatively, the passenger can pre-register (in a Registered Traveller Programme (RTP)). In that case, the biometric data can be stored on a central

database, as in the PARAFE programme for non-French citizens in France and the discontinued IRIS in the UK, or on a card as in the PRIVIUM system used at Schiphol in the Netherlands.

When data are automatically processed, as by ABC, certain privacy and data protection principles and provisions have to be observed. According to EU and national data protection laws, sensitive data enjoy stricter protection due to the higher risks they pose to individuals, for example inaccurate matching on the basis of which decisions against individuals could be taken.

Recommendations for handling personal data processed by ABC

Considering that ABC has implications for border agencies as controllers of personal data that is automatically processed, the processes should be compatible with the applicable data protection framework . Therefore, I propose some recommendations for ABC derived from Art. 8 European Convention of Human Rights (ECHR), Art. 7 and 8 Charter of Fundamental Rights of the EU (CFREU), Directive 95/46/EC on data protection, as well as the case-law of the Strasbourg and Luxembourg Courts.



They might make things faster, but are they adequately protecting out data?
photo by Terence T.S. Tam CC BY-NC-SA 2.0

As with the collection of any personal data, ABC should pursue a legitimate aim. It is argued that ABC is needed to speed up border control and reduce queues. Effective border management could be a legitimate goal for ABC. Still, the means to achieve it have to be (1) based in a law which is sufficiently precise to prevent against arbitrary (mis)use of the data; (2) necessary to achieve the aim, i.e. adequate to achieving the aim, not simply contributing towards it; and (3) proportionate, i.e. the least intrusive means of achieving the goal. This means that if there are other means to achieve effective border management, which entail fewer risks for passengers, these should be preferred. The purpose is to balance the risks for passengers against the benefits of the system.

Once the necessity and proportionality are motivated, the following non-exhaustive list of measures should be taken:

- A law on ABC with sufficient safeguards for passengers should be passed, as currently the SBC regulates border checks as performed by border guards, not by automated gates (See Articles 7 and 15). In addition, it has to be clarified in how far the e-Passport Regulation allows the processing of the biometric identifiers on the chip of the passport on a more regular basis (cfr AG opinion in *Schwarz*).
- For those using the Registered Travellers Programme, the enrolled biometrics should preferably be stored on a token in the possession of the traveller such as in the PRIVIUM system instead on a central database. If a database is established, verification (1:1 matching) should be preferred over identification (1:n matching) and verification should ensure accurate matching (data accuracy).
- The live biometrics presented for verification at the e-Gate should not be stored on a central database, as this might lead to function creep, if, for instance, the law enforcement authorities gain systematic

access to it a real and present interest, answering a pressing social need, should be demonstrated to access such data.
- The security of data procesed by ABC should be ensured against attacks such as hacking, eavesdropping, skimming.
- Clear information should be provided to all users about the processing of their data, including at least the identity of the controller, the purposes of the processing, categories of data, and how travellers can exercise their rights.

Thus, legislators should ensure a proper legal basis for ABC, while the responsible authorities for border checks should, as data controllers, ensure compliance with privacy and data protection principles and rules.

This post gives the views of the author, and does not represent the position of the LSE Media Policy Project blog, nor of the London School of Economics.

July 21st, 2014 | Guest Blog, Privacy | 0 Comments