Data Protection at the Schengen borders after Paris

Diana Dimitrova of the KU Leuven Centre for IT & IP Law discusses the proposed amendment from December 2015 to the Schengen Borders Code (SBC), tabled in response to the Paris attacks that took place in November 2015. In this post, she examines some of the privacy and data protection issues that arise from the provisions of the proposal.

The Schengen Borders Code

The Paris attacks in November 2015 triggered legislative changes at an EU level, especially measures focused on the process of border checks at the EU's external borders.

The Council, in its conclusions on 20 November 2015, appeared to echo some of the proposals made by the French delegation earlier as a tool to fight terrorism. In December 2015 the Commission tabled a proposed amendment of the Schengen Borders Code (SBC), translating the Council Conclusions into a legislative proposal. This proposed amendment seeks to address "the phenomenon of foreign terrorist fighters, many of whom are Union citizens" (Recital 2) and includes (1) a mandatory systematic database search on wanted individuals and on lost and stolen passports (the latter is not new) for European Union/European Economic Area/Swiss (EU/EEA/CH) citizens and (2) biometric verification when there is doubt concerning passport authenticity or passenger identity, pursuant to Council Regulation 2252/2004 (on biometric features in passports of EU/EEA/CH citizens).

On 3 February the Council provided its deliberations on the draft legislative text and proposed, amongst others, (1) the use of 'automatic border control gates' to speed up background database searches and (2) advance background checks using Advance Passenger Information (API) and other sources.

This blog will examine the proportionality of the proposed amendment in relation to security concerns at the Schengen borders and the data protection concerns that should be addressed.

Affected rights – privacy and data protection

The possible intrusion into the fundamental rights to privacy and data protection stems from the proposed processing of biometric data and the systematic (advance) background checks on all citizens who currently enjoy the right to freedom of movement in the EU (mainly EU/EEA/CH) and who are currently subject only to a minimum check and are non-systematically checked against databases of wanted persons. Notably, the proposed amendment to the SBC removes the term 'minimum check'.

Biometrics

The Commission proposed biometric verification for EU/EEA/CH citizens 'in case of doubts on the authenticity of the travel document or on the identity of its holder'.

Up until now, the SBC did not include provisions for the processing of biometric features in EU/EEA/CH passports at external borders. Thus, the clarification as to when EU/EEA/CH biometric features should be verified at borders is welcome. One interpretation is that there is no obligation to *systematically* verify the biometric features of *all* passengers, but rather only in individual cases of doubt.

Article 9 (1) of the December 2015 version of the proposed General Data Protection Regulation (GDPR) classifies biometric data as sensitive data when processed with the purpose of uniquely identifying a person, which evidently is the case in the border control context. Amongst the proposed legal bases for processing, Art. 9(2)(g) seems the most likely candidate in the discussed context. Pursuant to it, biometric data may be processed when this is *necessary* for a substantial public interest, if there is a legal basis which is *proportionate* to the aim pursued, respects the essence of the right to data protection and provides for suitable and specific safeguards.

These requirements mirror the provisions of Art. 7 and 8, in conjunction with Art. 52 (1) Charter of Fundamental Rights of the EU. Member States may introduce further requirements (Art. 9 (5)).

As to the legal basis, one could argue that Council Regulation 2252/2004, which introduced biometrics in passport chips of EU citizens (together with the proposed amendment to the SBC), constitutes a legal basis. The legal basis should be proportionate and fully address the risks of the technology, respecting the essence of the fundamental right. The GDPR explicitly calls for a Data Protection Impact Assessment ("DPIA") (Art. 33(2)(b)) when sensitive data, e.g. biometric data, are processed on a large scale. The Commission stated clearly that the GDPR should apply to areas such as border control. A comprehensive DPIA for this SBC amendment is necessary also because data processing for border control purposes should be re-examined through the lenses of privacy and data protection, which gained the status of fundamental rights in 2009.

The DPIA should assess the risks and propose adequate mitigating measures and safeguards to minimise the negative impact on passengers. Safeguards would be needed especially with regards to the accuracy of the conclusions of biometric verifications, false rejections, data abuse and illegal storage. In addition, passengers should be properly informed about the processing of their (sensitive) data and their rights as data subjects.

From a necessity and proportionality perspective, the question is whether biometric verification will effectively help fight terrorism. As explained in another LSE blog, biometric uniqueness cannot solve the fundamental problem of whether a person is who they claim they are. It can only confirm whether it is 'reasonably certain' that the person holding an ID document is the person to whom it was issued. A person could be a terrorist and still be the legitimate owner of a valid passport, obtained legally or *fraudulently*, e.g. by stealing genuine blank documents, as is claimed to happen in IS controlled areas. Biometric verifications will not solve *this* problem. They could be helpful in detecting a stolen passport only if it is not reported to be stolen and the database search cannot detect it.

In the aftermath of the Paris attacks, there has been speculation that some of the perpetrators were carrying fake passports. Thus, an essential measure in the fight against terrorists is complying with the mandatory systematic genuineness check. As biometrics are not the only way the genuineness can be checked, the proposed SBC amendment should not lead to a disproportionate usage of biometrics.

Background checks and "Automatic Border Control"

The Council has also proposed the introduction of automated border control (ABC) technologies (which are not specified but are presumably e-gates and kiosks), although it is not entirely clear for what purposes. One interpretation is that ABC can be used to save time by conducting all background checks in parallel. Although ABC is already widely used, it is currently not mentioned in any EU legal acts currently in force. The proposed SBC amendment gives the EU the opportunity to define the *scope, purposes and functions of ABC*, as well as to enshrine the necessary safeguards for passengers.

Since the proposed role of ABC is vague, this leads to uncertainty about the purposes it is introduced for and its scope, i.e. which processes it includes. If biometric verification is integrated into manual border control, could manual border control processes also fall within its definition? This concerns the distinction between manual and automated border control processes, and the

difference in the data processing and the ensuing privacy and data protection risks that both types of border controls pose. It is advisable that the aforementioned DPIA on biometric processing should take into account the context of any border control, without prejudice to the fact that ABC as such should be well defined and regulated.

As currently certain ABC programmes rely on passenger consent, an interesting question is whether in the future it will be possible to say that the use of ABC gates and the biometric data processed through it are legitimately based on passenger consent, in view of the fact that the distinction between ABC and manual control is becoming blurred.

As to the background checks, the change in the proposed amendment is the systematic background person check on EU/EEA/CH citizens. This is a departure from the current rule where EU/EEA/CH were checked only non-systematically. If the Council text is adopted, then API and other data, such as PNR data, might be used to perform these checks in advance and would be verified against the passport data at the border. While this might contribute to data accuracy, other potential data protection risks should be assessed and addressed.

Conclusion

This blog does not argue that technologies for border control are unable to address current security issues. Rather, it is vital that the appropriate technology and policy alternatives are chosen after the problem has been rigorously identified. The selected measures should be **necessary, proportionate and supported by stringent safeguards for individuals after a detailed DPIA analysis.**

This article 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. This piece reflects the personal opinion of the author and does not represent the views of the FastPass consortium.

March 14th, 2016 | Data Protection, EU Media Policy, Featured | 0 Comments