The Willems judgment: CJEU's missed chance to rein in biometric data usage

In her fourth post on data retention and border controls, ***Diana Dimitrova from KU Leuven*** *looks at the Court of Justice of the European Union's (CJEU) judgment in the Willems case. Diana discusses the Court's reasoning on the applicability of the Charter of Fundamental Rights of the EU (CFREU) to the further usage of the biometrics (facial and fingerprint images) collected and stored by Member States on the chip of EU biometric passports. She also argues why more safeguards for their use are necessary.*

The judgement

In the *Willems* judgment the CJEU was asked to rule, amongst other questions, on whether Article 4(3) of the e-Passport Regulation must be interpreted as requiring Member States to guarantee that the biometric data they collect and store pursuant to that Regulation will not be further used for purposes other than issuing the travel document. The applicants were concerned that upon collection the Dutch government stores the biometrics in a decentralized database, which could become centralized and the data could be accessed and reused by other entities, e.g. the law-enforcement.

The Court ruled that such re-use of the biometric data by Member States, which are collected to issue travel documents, falls outside the scope of that Regulation and by extension outside the scope of Union law. This leads to the inapplicability of the CFREU in cases of further use of the data by Member States. Consequently, Articles 7 and 8 of the CFREU on the rights to privacy and data protection do not apply.

However, the reasoning of the Court raises legal concerns, both regarding the applicability of the CFREU (also discussed by Eduardo Gill-Pedro and Steve Peers), and the necessity for regulation of the (further) usage of the biometric data stored on passport chips.

On the applicability of the CFREU

In par. 46 of *Willems* the Court recalls that in *Schwarz* it ruled that the storage *and usage* of the biometric data on the chip is compatible with Articles 7 and 8 of the CFREU. As a re-cap, in par. 36 and 37 of *Schwarz*, the Court concluded that Article 1(2) of the e-Passport Regulation, which requires the storage of biometric data on the chip, is compatible with the CFREU because it fulfills the requirements of Article 52 (1) of the CFREU. One of the requirements of the said Article is that an interference with fundamental rights, such as privacy and data protection, should "genuinely meet objectives of general interest recognized by the Union." The Court argued that the regulation's objective is "to prevent, inter alia, illegal entry into the European Union" which is subject to border checks at the external borders of the EU, regulated by the Schengen Borders Code (SBC) Regulation. It is part of the Union's policy on 'Border checks, asylum and immigration" (Article 77, Chapter 2, Title V Lisbon Treaty), which falls under the Area of Freedoms, Security and Justice (AFSJ). In pars. 170-172 of its Opinion 2/13, the CJEU clearly stated that the AFSJ contributes "to the implementation of the process of integration that is the *raison d'être* of the EU itself."

Member States collect and store biometrics on EU passports following a Union obligation, serving a Union policy. Thus, the data should not be used beyond this policy and beyond the purposes of the e-Passport regulation. In par. 66 of the Data Retention judgment the Court criticized the *Data Retention Directive* as it "does not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against

any unlawful access and use of that data." It would be logical that the further usage of the data collected to issue the passport, e.g. storage on a database and access by the law-enforcement to it, should be examined against the Charter and Directive 95/46/EC to ensure harmonized safeguards across the Member States.

Why harmonized safeguards about the (re)-use of chip data are necessary

Biometric applications are permeating more and more our lives. The applicants in *Willems* were concerned that governments can create a database of their biometrics which are collected when citizens apply for passports. However, technically governments can create such biometric databases also later, e.g. during the border control process if biometrics are used for verification purposes according to Article 4 (3) of the Regulation, although that was not an issue raised in *Willems*.

In the recent years there has been a trend amongst EU Member States to introduce more sophisticated technologies for border control at their external borders, e.g. technologies for Automated Border Control (ABC). Such technologies are designed to process the biometric data on the chip passport. A lot of ABCs process biometrics to verify the identity of the passenger through a 1:1 verification of the live biometrics presented at e-Gates against the biometrics stored on the chip. When it comes to EU citizens, the SBC does not as such require that the identity is established on the basis of *automated biometric verification.* Currently a *visual comparison* with the picture on the travel document suffices (except for visa-holders who are not EU citizens, however).

And this is why safeguards and limitations should be clearly articulated. For instance when the chip is opened, technically the facial image could be retrieved and stored. Fingerprints could be accessed too, but currently only by the government that issued the passport. Should governments be allowed to store the available biometrics from the passport chip on some kind of databases and further use them for purposes not related to border control? In the proposed Smart Borders Package, one of the proposals concerns the establishment of the Entry Exit System, according to which all Third Country Nationals (TCNs) who visit the EU on a short stay would be required to provide 10 fingerprints, which would be stored on a central, EU-wide database for administrative purposes. The original proposal also envisaged that this database could be accessed systematically by law-enforcement authorities, which is a deviation from the original purpose.

Conclusions

While this proposal incurred a lot of criticism on the necessity and proportionality of such a measure and its compatibility with Articles 7 and 8 CFREU, EU citizens' data deserve no less protection. If rules on border control are being harmonized on EU level, then so should be the level of protection of the data of passengers who cross borders at different Member States' external borders. And it is surprising the Court did not discuss the applicability of Directive 95/46/EC to the further usage of biometrics, as Steve Peers comments.

Member States store biometric data on the passport chip pursuant to the e-Passport regulation to prevent illegal entry into the Union, which is intimately tied to the EU policy of external border control. Following the *Data Retention* Judgment, the CFREU should also apply to the potential further processing of the biometric data which Member States collect to issue passports, e.g. re-use for law-enforcement purposes, in order to prevent illegal use of the data. Similarly, Art. 4(3) of the e-Passport regulation provides for the usage of the biometrics to verify the authenticity of the passport or the identity of the individual, e.g. during border checks. This processing of biometrics also offers opportunities for re-use. The scope of its lawful processing should then be better defined according to the principles in the Charter and Directive 95/46/EC either in the e-Passport Regulation or in other relevant legislations, e.g. the Schengen Borders Code.

This piece reflects the personal opinion of the author and does not represent the views of the FastPass consortium, nor the position of the LSE Media Policy Project blog or the London School

of Economics.

September 9th, 2015 | EU Media Policy, Featured, Privacy | 0 Comments