



Biometric data and data protection law: the CJEU loses the plot

Steve Peers, Professor of Law, University of Essex

Many people are increasingly concerned about adequate protection of their biometric data. To this end, the proposed EU data protection [Regulation](#) would classify that data as sensitive data, ensuring an extra degree of protection for it. But in the meantime, before that proposal is adopted, there are other EU measures which regulate the issue. Unfortunately, yesterday's [judgment](#) of the CJEU in *Willems and others* does an inadequate job, with great respect, in applying the current EU rules to such data.

Background

The *Willems* judgment concerns biometric data collected for passports, as provided for in an EU [Regulation](#) of 2004, as [amended](#) in 2009. In fact, the CJEU has ruled on this Regulation several times before. In *UK v Council*, it (unconvincingly) [ruled](#) that the UK could not participate in the Regulation, since it was closely linked to the parts of Schengen rules (the abolition of internal border controls) in which the UK didn't participate. In *Schwarz*, it [ruled](#) that the Regulation was valid from two different angles, as it was correctly adopted using the 'legal base' allowing the EU to adopt measures on external border control, and the interference which it entailed with the right to privacy was justified by the interest in ensuring the identity of passport holders and the validity of the passport. Finally, the Court recently ruled on the privacy aspects of displaying names in passports (as discussed [here](#)).

Building on these judgments, the national court in *Willems* had two questions. First of all, did the Regulation apply to some types of identity cards, given that they can in effect be used as passports for travel within the EU? Secondly, the national court asked the CJEU to interpret the data protection rules applicable to the further use of biometric data after it was collected for the purposes of passports. The latter question stemmed from the concern of the litigants in this case that their biometric data would be stored on a centralised database with inadequate security, which would be used for other purposes without a clear identification of who would have access to it.

More precisely, the national court's second question was whether 'Article 4(3) of [the passport Regulation, read] in light of Articles 7 and 8 of the Charter of Fundamental Rights of the [EU], Article

8(2) of the [ECHR] and Article 7(f) of [the current data protection [Directive](#)], read in conjunction with Article 6(1)(b) of that Directive', required a guarantee that when collecting biometric data under the Regulation, Member States had to apply a 'purpose limitation' rule that such data could only be used for the original purpose for which the passport was issued.

Judgment

On the first question, the CJEU looked at the wording of the Regulation, which specified that it did not apply to 'identity cards issued to [Member States'] nationals or to temporary passports and travel documents having a validity of 12 months or less'. The Court ruled that the words 'having a validity of 12 months or less' only set out the scope of the Regulation as regards 'temporary passports and travel documents', meaning that such documents *were* within the scope of the Regulation if they were valid for more than 12 months. On the other hand, the words 'having a validity of 12 months or less' did *not* set out the scope of the Regulation as regards national identity cards. So no identity cards fall within the scope of the Regulation, regardless of the period of their validity.

On the second question, the CJEU ruled that the passport Regulation only governed the use of data for the purposes of that Regulation. Any further use of that data, as specified in the preamble, was regulated by national law. It followed that the Regulation did not apply a purpose limitation rule upon Member States as regards biometric passport data. Because the Regulation did not apply to such uses by Member States, the EU Charter did not apply either, although such further use of data might be restricted by national law or the ECHR. Finally, as for the data protection Directive, the CJEU stated that 'the referring court was requesting the interpretation of [the passport Regulation] and only that Regulation', so there was no need to examine whether the data protection Directive affected national law on the further storage and use of biometric data collected for passport purposes.

Comments

I won't mince words: this judgment is appalling. It's sensible enough as regards the scope of the passports Regulation itself, which clearly wasn't intended to apply to any national identity cards or to the creation of government databases using biometric data. But the Court's fundamental flaw is its failure to confirm and elaborate upon the application of the Charter and the data protection Directive to such databases.

Let's examine those two points in turn. As regards the Charter, of course it's true, as the Court says, that it only applies when a dispute falls within the scope of EU law. But the Court made that point only as regards the scope of the passports Regulation, *before* (not) answering the question about the data protection Directive. Logically the Court cannot conclude that this dispute is not linked to EU law before it assesses also whether the data protection Directive applies.

Anyway, if we apply the Court's own case law, the link to the passports Regulation *alone* brings this issue within the scope of the Charter. In *NS*, a key [judgment](#) on the scope of the Charter, the EU's Dublin Regulation left an option to Member States to decide *in their national law* whether to consider asylum applications which fell within the responsibility of another Member State. But the Court ruled that the Charter applied to such national discretion. More relevantly, in a line of cases starting with [Promusicae](#), the Court applied the Charter in detail to a national *option* to provide for the collection of personal data on use of the Internet set out in EU law. And in last year's *Digital*

Rights judgment, the Court invalidated the EU's data retention Directive for the very reason that this Directive failed to effectively regulate the further national use of personal data collected pursuant to it.

As regards the question about the data protection Directive, the CJEU's answer simply departs from reality. It is quite clearly *not true* that the national court was 'only' asking for an interpretation of the passport Regulation. As we can see from the text of the question excerpted above, it also asked the CJEU to interpret the data protection Directive. Admittedly, it only asked the CJEU to interpret the Directive in the *context* of the Regulation. But the CJEU does not make that distinction clear; and more importantly, that distinction *just doesn't matter*.

Why? Because the CJEU has frequently rephrased questions by national courts in order to give a full reply to the EU law issues which they are actually having to address in the relevant litigation. The examples are legion, but the most relevant one is the judgment in *Promusicae*. In that case, which concerned mass interception of Internet users' activity for the purposes of enforcing intellectual property rights, the national court only asked questions about EU intellectual property law and the e-commerce Directive. The CJEU quite rightly redrafted the questions in order to give an answer about the relevant data protection rules (in that case, the e-privacy Directive) as well. In *Willems*, the national court had already identified the relevance of the data protection Directive, so a comparatively minor redraft of its questions would have sufficed in order to ensure a reply that was fully relevant to the national litigation.

The Court's ruling is also unsatisfactory in the broader context of the legislation and case law on similar issues. When it asserted that national law applied to databases of biometric data, the CJEU only selectively quoted from the preamble to the passports Regulation. Recital 4 of the preamble to the 2004 Regulation states that access to the data collected as regards biometric passports is 'subject to any relevant provisions of [EU] law'. Moreover, the CJEU interpreted the data protection Directive as regards a comparable national database (a collection of information on foreign nationals) in the [Huber](#) judgment. I should note that the data protection Directive also applies where the passport Regulation does not: to biometric information collected as regards identity cards, and to passport biometric information collected in the Member States that are not bound by the Regulation (the UK and Ireland). Finally, the Court's indifference to the fate of biometric data collected by Member States as regards passports seriously undercuts its own ruling in *Schwarz*, when it defended the validity of the passports Regulation on the basis of the limited scope of its interference with privacy rights (proportionality), and quoted the *S and Marper* judgment of the European Court of Human Rights to the effect that 'the [EU] legislature must ensure that there are specific guarantees that the processing of such data will be effectively protected from misuse and abuse'.

At first sight, these criticisms of the ruling may seem legalistic. But my concerns are about much more than the deep flaws in the Court's legal reasoning here. As we all know, the scope of databases and mass surveillance of individuals ('big data') have increased exponentially in recent years. This raises huge human rights issues and EU law has a significant role to play. Last year, in its judgments in *Digital Rights* and *Google Spain*, the CJEU genuinely tried to grapple with these issues. Many aspects of these judgments have been criticised, but the Court is at its best when it fully engages in these important legal debates. When it avoids them, with the specious legalism it spouts in *Willems*, it is at its worst.

This article first appeared in EU Law Analysis

March 2015