Safe Harbour: Key Aspects of the ECJ Ruling

Today, the Court of Justice of the European Union (ECJ) declared that the Safe Harbour agreement which allowed the movement of digital data between the EU and the US was invalid. The Court was ruling in a case brought by Max Schrems, an Austrian student and privacy campaigner who, in the wake of the Snowden revelations of mass surveillance, contested the fact that data about Europeans and others was being stored in the US by tech companies such as Facebook. Professor Lorna Woods of the University of Essex explains some key aspects of the judgment.

This case arises from a challenge to the transfer of personal data from the EU (via Ireland) to the United States, which relied on a Commission Decision 2000/520 stating that the Safe Harbour system in place in the United States was 'adequate' as permitted by Article 25 Data Protection Directive. While the national case challenged this assessment, the view of the Irish data protection authority (DPA) was that it had no freedom to make any other decision – despite the fact that the Irish authorities and courts were of the view the system did not meet the standards of the Irish constitution – because the European Commission decision was binding on them. The question of the validity and status of the Decision were referred to the Court of Justice of the European Union (ECJ).

The Advocate General, a senior ECJ official who advises on cases, took the view that the Commission's decision could not limit the powers of DPAs granted under the directive and that the US system was inadequate, particularly as regards the safeguards against mass surveillance (a more detailed review of the AG's Opinion can be found here). The ECJ has now ruled, following very swiftly on from the Opinion. The headline: the Commission's decision is invalid. There is more to the judgment than this.

Powers of DPAs and Competence

The ECJ emphasised that the Commission cannot limit the powers granted by the Data Protection Directive, but at the same time Commission decisions are binding and benefit from a presumption of legality. Nonetheless, especially given the importance of the rights, individuals should have the right to be able to complain and ask a DPA to investigate. DPAs remain responsible for oversight of data processing on their territory, which includes the transfer of personal data outside the EU. The ECJ resolves this conundrum by distinguishing between the right and power of investigation and challenge to Commission decisions, and the declaration of such decisions' invalidity. While the former remains with DPAs, the latter – following longstanding jurisprudence, remains with the ECJ.

Validity of Decision 2000/520

The ECJ noted that there is no definition of what is required by way of protection for the purposes of Article 25 of the Data Protection Directive. According to the ECJ, there were two aspects to be derived from the text of Article 25. There is the requirement that protection be 'adequate' in Article 25(1) and the fact that Article 25(6) refers to the fact that protection must be ensured. The ECJ agreed with the Advocate General that this Article is 'intended to ensure that the high level of that protection continues where personal data is transferred to a third country' (para [72], citing the Advocate's General's Opinion para [139]), which seems higher than 'adequate' might at first suggest. That requirement does not however mean that protection in third (non-EU) countries must be identical but rather that it is equivalent (para 73]) and effective (para [74]). This implies an on-going assessment of the rules and their operation in practice, where the Commission has very limited room for discretion.

The Court concluded that the Decision was unsound. It did so on the basis that mass surveillance is unacceptable, that there was no legal redress and that the decision did not look at the effectiveness of enforcement. It steered clear of determining whether the self-certification system itself could ever be fit for purpose, basing its reasoning on only elements of the Commission's decision (but which were so linked with the rest that their demise meant the entire decision fell).

Implications

This is a judgment with very far reaching implications, not just for governments but for companies the business model of which is based on data flows. It reiterates the significance of data protection as a human right, and underlines that protection must be at a high level. In this, the ECJ is building a consistent line of case law – and case law that deals not just with mass surveillance (*Digital Rights Ireland*) but activities by companies (*Google Spain*) and private individuals (*Rynes*).

At a practical level, what happens today with the Decision declared invalid? Going forward, will there be more challenges looking not just at mass surveillance but at big data businesses self-certifying? What will happen to uniformity in the EU? Different Member States may well take different views. This should also be understood against the *Weltimmo* judgment of last week, according to which more than one Member State could have the competence to regulate a multinational business (irrespective of where that business has its registered office in the EU). Finally, what does this mean for the negotiation of the Data Protection Regulation? The political institutions had agreed that the Regulation would not offer lower protection than the Data Protection Directive, but now we might have to examine this directive more closely.

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 and Political Science.

October 6th, 2015 | Data Protection, EU Media Policy, Featured, Privacy | 2 Comments