# Safe Harbor in the dock

The Court of Justice of the European Union may consider the validity of the whole US Safe Harbor arrangement.
By **Eduardo Ustaran**.

The fact that the Safe Harbor framework is permanently in the firing line is not particularly earth-shattering, but the prospect of the top European court declaring its inadequacy later this year could have dramatic consequences. This prospect became all the more possible after a hearing at the Court of Justice of the European Union ('CJEU') in Luxembourg in March. Safe Harbor was the end result of several years of negotiations during the late 90s between the European Commission and the US Department of Commerce to create a

*Continued on p.4*

*Safe Harbor... from p.1*

self-regulatory framework that would allow US-based organisations to overcome the restrictions on transfers of personal data from the EU. The Safe Harbor agreement was a remarkable achievement which has facilitated legal compliance for the past 15 years.

However, since its adoption, Safe Harbor has been fraught with challenges. Although the data protection requirements set out in the Safe Harbor Privacy Principles are meant to match the adequacy standards of the European data protection directive, its self-certification nature and the non-European style of its provisions have attracted much criticism over the years – even amongst EU data protection authorities. Whether such criticism is founded on an objective assessment of Safe Harbor or just gut-instinct is debatable but the situation in which Safe Harbor finds itself today was rather predictable.

## The Snowden effect

The revelations triggered by Edward Snowden in 2013 about the mass surveillance operations carried out by the NSA had a very visible knock-on effect on the way in which the EU regulates international transfers of personal data. Activists' calls for the revocation of the Safe Harbor framework led the European Parliament to adopt a resolution seeking its immediate suspension. As a result, the European Commission – always measured and pragmatic – had no choice but to reopen the dialogue with the US government to find a way of strengthening the framework and restoring its credibility.

One particular individual, Austrian law student Max Schrems, decided not to wait for the outcome of the renegotiation of Safe Harbor. Following the Snowden revelations, he lodged a complaint with the Irish Data Protection

 

Commissioner requesting the termination of any transfers of personal data by Facebook Ireland to the US. Schrems claimed that Facebook Ireland – the data controller for Facebook's European users' data – could no longer rely on Safe Harbor to legitimise the transfers of his data to the US because of the wide access that US authorities had to such data as revealed by Snowden.

However, the Irish Commissioner rejected the complaint on the basis that the adequacy of Safe Harbor had already been determined by the European Commission and therefore, it was not open to the Irish Commissioner to challenge the European Commission's 'adequacy finding'. This was not accepted by Schrems who remained adamant that the Safe Harbor framework did not provide an adequate level of protection for his data. Therefore, Schrems took the unprecedented step of seeking judicial review of the Commissioner's decision.

## In the hands of the CJEU

Throughout the EU, the decisions of the Data Protection Authorities may be challenged in court. In the case of the Irish Data Protection Commissioner, the High Court of Ireland is the competent tribunal for these purposes and the forum where Schrems sought relief by requesting that the Commissioner's rejection be overturned. The High Court took the view that the main issue at stake was a matter of EU law. The High Court explained that whilst the Commissioner was indeed able to direct an entity to suspend data flows to a third country declared adequate by the European Commission, this was only in circumstances where – unlike in this case – the complaint was directed to the conduct of that entity.

Therefore, the High Court considered that what needed to be determined was whether the Irish Data Protection Commissioner was absolutely bound by the Safe Harbor adequacy finding, which is, a matter of EU law. In other words, the High Court considered that Schrems' real objection concerned not the conduct of Facebook Ireland as such, but the fact that the European Commission had determined that Safe Harbor provided adequate protection for data exported from the EU in the light of the disclosures made by Edward Snowden regarding access of EU citizens' data by the US authorities. Since this is a matter of interpretation of the EU data protection legal framework, the High Court referred this particular point for decision by the CJEU.

The CJEU held its first and only public hearing of this case on 24 March 2015. Schrems' main argument was that the European Commission's Safe Harbor adequacy finding should be declared invalid because of its incompatibility with both the EU Data Protection Directive and the Charter of Fundamental Rights of the EU. Schrems made a comparison with the CJEU's own decision on the data retention directive and argued that the interference caused by the interception and surveillance of European citizens' data under Safe Harbor was even more serious. For this reason, Schrems urged the CJEU to question the validity of Safe Harbor as a whole, even though the specific questions referred by the High Court of Ireland did not formally concern such validity.

Schrems went on to argue that at the very least the Irish Data Protection Commissioner had the overriding duty to protect the fundamental right to privacy and that the Commissioner's competence must be interpreted in light of this objective. Furthermore, Schrems argued that it would be contrary to the independence of Data Protection Authorities if those authorities were absolutely bound by the European Commission's adequacy decisions.

The Irish Data Protection Commissioner's position was quite simple: Data Protection Authorities' powers are limited by the national laws that establish their office, and as such, those authorities cannot strike down national laws, EU directives or the acts enabled by those directives and laws. The Commissioner also seemed alarmed that Schrems was seeking to go beyond the questions referred by the High Court and question the validity of Safe Harbor altogether. Ultimately, Safe Harbor was a framework negotiated by the European Commission and therefore, it was not up to the Irish Commissioner to disregard that compromise. The lawyers acting for the Irish Government, which also made representations at the hearing put forward the same argument.

Other countries and EU institutions represented at the hearing included Belgium, Austria, Poland, Slovenia, the UK, the European Parliament, the European Commission and the European Data Protection Supervisor. Of those, only the UK government and the European Commission sided with the Irish Data Protection Commissioner. The Austrian government's comments were particularly scathing as its representative reportedly said that "Safe Harbor is just a safe harbor for data pirates". Similarly heated arguments were made by representatives from the European Parliament who argued that the Safe Harbor presented "systematic inefficiencies" which could not be avoided.

## What next?

The CJEU has certainly much to mull over. Before a decision is made by the CJEU, the Advocate General's Opinion is due on 24 June 2015. This Opinion is not binding on the CJEU but it will give an indication of a possible outcome. A final decision will probably be made by the end of the year. There are a number of positions that the CJEU could take:

- Agreeing with the Irish Data Protection Commissioner and confirming the duty of the EU Data Protection Authorities to be bound by the European Commission's adequacy decisions – this would be in direct contradiction with the points made by a number of government delegations which argued strongly in favour of the ultimate decision-making power of the regulators.
- Simply answering the questions referred by the High Court of Ireland by confirming Schrems' arguments that it is possible for a data protection authority to challenge an adequacy finding made by the European Commission – this would not require much interpretative effort by the CJEU given the strong emphasis on the independent role of data protection authorities and that they are already entitled to question such adequacy findings in some cases.

- Going beyond the questions referred by the High Court of Ireland and taking a formal view on the validity of Safe Harbor – This would be a very bold move that would have serious political and economic implications, but that in itself will not be a deterrent for the CJEU.

To complicate matters, in parallel to the proceedings and deliberations taking place at the CJEU, the European Commission is progressing its negotiations with the US government on an updated Safe Harbor framework. The outcome of these negotiations may well be a determining factor in the CJEU's final decision. What seems clear is that it is of crucial importance for the future of Safe Harbor and the regulation of international data transfers that the European Commission manages to demonstrate beyond reasonable doubt that the protections afforded by Safe Harbor going forward are in line with the expectations of regulators, Member States and indeed the CJEU.

**AUTHOR**

Eduardo Ustaran is a partner in the global Privacy and Information Management practice at Hogan Lovells based in London.
Email: eduardo.ustaran@hoganlovells.com

# Join the Privacy Laws & Business community

## Six issues published annually

### PL&B's International Report will help you to:

**Stay informed of data protection legislative developments in 100+ countries.**

**Learn from others' experience through case studies and analysis.**

**Incorporate compliance solutions into your business strategy.**

**Find out about future regulatory plans.**

**Understand laws, regulations, court and tribunal decisions and what they will mean to you.**

**Be alert to future privacy and data protection law issues that will affect your organisation's compliance.**

## Included in your subscription:

**1. Online search functionality**
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

**2. Electronic Access**
You will be sent the PDF version of the new issue on the day of publication. You will also be able to access the issue via the website. You may choose to receive one printed copy of each Report.

**3. E-Mail Updates**
E-mail updates help to keep you regularly informed of the latest developments in data protection and privacy issues worldwide.

**4. Back Issues**
Access all the *PL&B International Report* back issues since 1987.

**5. Special Reports**
Access *PL&B* special reports on Data Privacy Laws in 100+ countries and a book on Data Privacy Laws in the Asia-Pacific region.

**6. Events Documentation**
Access International and/or UK events documentation such as Roundtables with Data Protection Commissioners and *PL&B Annual International Conferences*, in July, in Cambridge, UK.

**7. Helpline Enquiry Service**
Contact the *PL&B* team with questions such as the current status of privacy legislation worldwide, and sources for specific issues and texts. This service does not offer legal advice or provide consultancy.

## To Subscribe: www.privacylaws.com/subscribe

"*PL&B's International Report* is a powerhouse of information that provides relevant insight across a variety of jurisdictions in a timely manner. **Mark Keddie, Chief Privacy Officer, BT Retail, UK**"

## Subscription Fees

**Single User Access**

*International* Edition **£500 + VAT***

*UK* Edition **£400 + VAT***

*UK & International* Combined Edition **£800 + VAT***

* VAT only applies to UK based subscribers

**Multi User Access**

Discounts for 2-4 or 5-25 users – see website for details.

**Subscription Discounts**

Special charity and academic rate:
50% discount on all prices. Use HPSUB when subscribing.

Number of years:
2 (10% discount) or 3 (15% discount) year subscriptions.

**International Postage (outside UK):**

Individual International or UK Edition
Rest of Europe = £22, Outside Europe = £30

Combined International and UK Editions
Rest of Europe = £44, Outside Europe = £60

## Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.

*Privacy Laws & Business* also publishes the United Kingdom Report.
**www.privacylaws.com/UK**