"Reports of my death have been greatly exaggerated": The Advocate General's opinion in the *Max Schrems v. Facebook* case

By Cecilia Álvarez Rigaudias* and Natascha Gerlach**

October 1, 2015

On September 23, 2015, the Advocate General (AG) of the European Court of Justice (ECJ), Yves Bot, issued his long-awaited Opinion[1] in the *Max Schrems vs. Facebook* case.

In a nutshell, the AG opined that the European Commission's Safe Harbor adequacy decision regarding transfers of personal data to the United States does not prevent a Data Protection Authority (DPA) from investigating a complaint alleging inadequate protection of the data transferred under Safe Harbor and, where appropriate, from suspending the transfer of that data. In addition, Mr. Bot also proposed that the 15-year old Safe Harbor adequacy decision itself is no longer valid.

Background

Max Schrems, an Austrian citizen and Facebook user since 2008, filed a complaint with the Irish DPA challenging the transfer of personal data from Facebook Ireland to Facebook USA under Safe Harbor. Mr. Schrems claimed that his fundamental privacy rights are not sufficiently protected by the U.S. and data transfers made to it under Safe Harbor. As evidence, Mr. Schrems pointed to revelations made by

---

* Cecilia Álvarez Rigaudias is the European Privacy Officer Lead of the pharma multinational Pfizer. Cecilia is Vice-president of APEP (Spanish Privacy Professional Association), Spanish member of CEDPO (Confederation of European Data Protection Organisations) and member of the Steering Committee of The Sedona Conference Working Group 6.

** Natascha Gerlach is the Managing Attorney for EU Litigation Operations with Cleary Gottlieb Steen & Hamilton, currently based in their Brussels office. She oversees Cleary's European Practice Support Department, which supports the eDiscovery needs of all European offices. Natascha specializes in Data Protection issues in connection with cross-border discovery and advises on data security issues. She is a member of The Sedona Conference Working Group 6.

[1] The full text of the Opinion may be found at http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=req&docid=168421&occ=first&dir=&cid=328810. For a summary of the Opinion, *see* Court of Justice of the European Union, Press Release 106/15 (23 September 2015), at http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-09/cp150106en.pdf.

Edward Snowden concerning the activities of U.S. intelligence, and in particular, the National Security Agency (NSA) "PRISM" program, with its unrestricted access to mass data stored on servers in the U.S., including Facebook USA's servers.

The Irish DPA rejected his complaint, holding that the European Commission's Decision "2000/520/EC on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce" was binding and prevented it from investigating the complaint further. Mr Schrems brought proceedings before the Irish High Court for judicial review of the Irish DPA's decision. The Irish High Court in turn decided to stay proceedings and refer the following question to the ECJ for clarification: whether, in the course of determining a complaint that personal data is being transferred to a third country (in this case, the U.S.), the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, an EU DPA is absolutely bound by an adequacy decision of the European Commission (in this case, the U.S. Safe Harbor decision) or, alternatively, whether it must conduct its own investigation of the matter in the light of factual developments in the time since the adequacy decision was first published?[2]

The Opinion

As is customary in such cases, the ECJ's AG weighed in with an opinion. The AG provided his views concerning two issues:

i. the powers of national DPAs to investigate and suspend international data transfers after receiving a complaint concerning transfer of personal data to an undertaking established in a third country and claiming an adequate level of protection of the data transferred, despite an existing adequacy decision by the European Commission (such as the U.S. Safe Harbor decision); and

ii. the validity of the Safe Harbor system contained in the European Commission's July, 2000 adequacy decision, which was not a question posed by the Irish High Court.

Powers of national DPAs

The AG stated that a decision by the European Commission on the adequacy of the level of data protection provided by a country outside of the EU does not eliminate or reduce the powers granted to the DPAs under the EU Data Protection Directive. Despite being generally legally bound by a Commission decision, national DPAs

---

[2] *Maximillian Schrems v. Data Protection Commissioner*, Case C-362/14 (European Court of Justice, July 25, 2014)(Reference for a preliminary ruling from High Court of Ireland), available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=157862&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=191188.

have, in the AG's opinion, the power to investigate international transfers of personal data where a complaint is lodged, even where such an adequacy decision (such as the U.S. Safe Harbor decision) exists, and cannot summarily reject such a complaint based merely on the existence of the adequacy decision.

In a case where systematic deficiencies in the level of data protection provided by the country to which the personal data is transferred have come to light, the DPAs must be able to:

i. carry out their investigations and, where appropriate, suspend the transfer of data; and

ii. bring matters before their national court, which will be able to decide, where appropriate, to request preliminary rulings from the ECJ for the purpose of assessing the validity of European Commission adequacy decisions.

German DPAs essentially followed this approach back in 2013 when, in light of the surveillance activities by U.S. intelligence and security agencies, they decided to:

i. stop issuing approvals for international data transfers until the German government demonstrates that unlimited access to German citizens' personal data by foreign national intelligence services comports with the fundamental principles of data protection law (i.e., necessity, proportionality, and purpose limitation); and

ii. review whether to suspend data transfers carried out pursuant to the Safe Harbor Agreement and EU standard contractual clauses.[3]

Validity of U.S.-EU Safe Harbor Framework

Although it was not a question specifically referred to the ECJ by the Irish Court, the AG also concluded that the ECJ should render a decision on the validity of the 2000/520/EC Safe Harbor adequacy decision.

The AG stated that it is apparent from the findings of the Irish High Court and the European Commission itself that current law and practice in the U.S. permits large-scale collection of EU citizens' personal data, without providing effective judicial protection to EU citizens, as evidenced by, inter alia, the European Commission's current negotiations for updated Safe Harbor principles.

In his view, these findings demonstrate that the Safe Harbor decision does not contain sufficient guarantees for two main reasons:

---

[3] *See* Hunton & Williams LLP, "German DPAs halt data transfer approvals and consider suspending transfers based on Safe Harbor, EU model clauses" (July 23, 2013), http://www.lexology.com/library/detail.aspx?g=742ff712-8545-4c7d-9f20-3cf5b0fa5c4f.

i. Under the Safe Harbor decision, the adherence to the Safe Harbor framework may be limited: "*(a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case-law that create conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization*."[4]

   Because this wording is too general, the implementation of those derogations by the U.S. authorities is not limited to what is strictly necessary and constitute a disproportionate interference with the fundamental rights of EU citizens.

ii. EU citizens have no appropriate remedy against the processing of their personal data for purposes other than those for which it was initially collected and then transferred to the US.

   In particular, there is no independent authority capable of verifying that the implementation of the derogations from the Safe Harbor principles is limited to what is strictly necessary. Neither the Federal Trade Commission (FTC) nor private dispute resolution bodies have the power to monitor possible breaches of principles for the protection of personal data by public actors such as the U.S. security agencies. The Federal Intelligence Surveillance Court does not offer an effective judicial remedy to citizens of the EU whose personal data is transferred to the U.S., since protection against surveillance by government services provided for in U.S. law applies only to U.S. citizens and to foreign citizens legally resident on a permanent basis in the U.S. As also stated by the Commission, EU citizens cannot obtain access to, rectification of, or erasure of data; or administrative or judicial redress with regard to collection and further processing of their personal data taking place under the U.S. surveillance programmes.

On these bases, the AG concluded that the ECJ must declare the Safe Harbor adequacy decision is no longer valid.

What's next?

The Advocate General's Opinion is not legally binding and the current Safe Harbor adequacy decision remains a valid transfer mechanism at least until the ECJ makes its final ruling. This is expected as early as October 6.

[4] Annex 1 of the Safe Harbor decision.

Statistically, the ECJ confirms the AG's opinions in about 80% of cases. However, it remains to be seen whether the ECJ will reach the same conclusions as the AG on the powers of the national DPAs, and also lean further out the window by commenting on the validity of the current U.S.-EU Safe Harbor Framework. After the ECJ has issued a final judgment, the *Max Schrems v. Facebook* case itself will be remanded to the Irish High Court for further proceedings in accordance with the ECJ's ruling.

If the ECJ were to confirm the AG's Opinion, it would open the door to any of the 28 national DPAs scrutinizing—and even potentially suspending–international transfers, based on any adequacy decision made by the European Commission. There is nothing to say this would stop at Safe Harbor. It could potentially also be extended to Standard Contractual Clauses, Binding Corporate Rules, and decisions concerning individual countries. After several years of intense work on a new General Data Protection Regulation (GDPR) with the expressed aim of harmonization and a common approach to data protection in Europe, an ECJ confirmation of the AG's Opinion could be counterproductive and has the potential to create immense legal uncertainty.[5]

What is certain is that this Opinion will increase the pressure on the U.S. and EU government authorities to reach agreement on a revised U.S.-EU Safe Harbor Framework, and in particular on the derogations for national security and law enforcement. The pressure will intensify if the ECJ confirms the Opinion. The Opinion may also challenge the compromise recently reached--within the negotiations of the GDPR--regarding the deletion of the sunset clause invalidating Safe Harbor and current standard contractual clauses proposed earlier by the European Parliament.

The U.S. and the European Commission have recently finalized an "Umbrella Agreement" on law enforcement sharing of information which would provide safeguards and guarantees that will ensure that EU citizens' personal data are protected when exchanged between police and criminal justice authorities. Implementation of the agreement is dependent on two steps:

i. The enactment of legislation in the U.S. that gives EU citizens the same judicial redress rights as U.S. citizens in the event of privacy breaches, which is one of the main arguments used by the AG for considering the Safe Harbor Framework to be no longer valid. A Bill

---

[5] *See also* Omar Tene, Let Justice Pierce the Mountain," (Sept. 25, 2015), https://iapp.org/news/a/let-justice-pierce-the-mountain/.; Christopher Kuner, "Safe Harbor in stormy seas: The Advocate General Opinion in Schrems," (Sept. 29, 2015) http://cjicl.org.uk/2015/09/29/safe-harbor-in-stormy-seas-the-advocate-general-opinion-in-schrems/.

on Judicial Redress was introduced in the U.S. Congress in March 2015.[6]

ii. The European Parliament's consent: the decision to conclude the agreement will be taken by the European Council but is subject to the European Parliament's consent.

This has limited application in the private sector, where Safe Harbor applies, but it may also be a consideration finding its way into the ECJ's final decision.

While the European Commission does not comment on ongoing ECJ cases, it stays committed to the ongoing negotiation for an updated Safe Harbor agreement with the U.S. It remains to be seen how an updated adequacy decision will fare under DPA scrutiny and whether the ECJ will comment on that eventuality.

* * *

[6] H.R. 1428, the "Judicial Redress Act of 2015," was approved by the House Judiciary Committee and referred to the full House on September 17, 2015 for a vote. *See* https://www.congress.gov/bill/114th-congress/house-bill/1428.