Bloomberg BNA

Privacy and Security Law Report®

Safe Harbor Program

Regardless of the possibility of a new trans-Atlantic data transfer pact to replace the invalidated Safe Harbor Program, companies must be prepared to use other solutions after assessing which are viable and carry the least risk, the authors write.

The Impact of the Court of Justice of the EU's Judgment Declaring The European Commission's EU-U.S. Safe Harbor Decision Invalid

By Cameron F. Kerry and William Long

Cameron F. Kerry, senior counsel at Sidley Austin in Boston, is the former general counsel and acting secretary of the Department of Commerce, where he led the Obama Administration's work on consumer privacy, including its engagement with the European Union on Safe Harbor and data protection.

William Long, a partner in Sidley's London office working on international privacy issues, was previously in-house counsel to one of the world's largest international financial services groups.

The decision by the Court of Justice of the European Union (the **CJEU**) on Oct. 6, 2015 invalidating the European Commission's EU-U.S. Safe Harbor Decision[1] (the **Judgment**) is a landmark judgment (14 PVLR 1825, 10/12/15). By voiding the legal basis for transatlantic data transfers for the 4,400 companies reliant on EU-U.S. Safe Harbor, the Judgment has unleashed vast legal uncertainty which is likely to remain a key concern to affected companies, data protection authorities (**DPAs**) and governments well into 2016. Further, by empowering DPAs to review adequacy decisions[2] independently of the European Commission, the Judgment ensures that these uncertainties will endure beyond the time it takes to adjust to the invalidation of Safe Harbor.

Of immediate importance for all affected companies and regulators is the statement issued on Oct. 16, 2015 by the Article 29 Working Party (the **Working Party**), the data protection advisory body composed of representatives from the national DPAs, the European Data Protection Supervisor and the Commission (14 PVLR 1940, 10/26/15). The statement announced a grace pe-

[1] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650

[2] Transfers of personal data to countries outside the European Economic Area may not take place under the Directive unless the recipient third country provides an adequate level of protection for the rights and freedoms of data subjects. The Commission under Article 25(6) of the Directive can make a finding of adequacy in respect of a third country by reason of its domestic law or the international commitments it has entered into. In addition, under Article 26(4) the Commission has the power to approve transfers of personal data made on the basis of certain standard contractual clauses which are deemed by the Commission to provide adequate safeguards for the rights and freedoms of data subjects.

 ISSN 1538-3423

riod until the end of January 2016 during which DPAs will not initiate coordinated enforcement actions against affected companies failing to implement appropriate data transfer mechanisms.

In the meantime, both the European Commission and its counterpart in the Safe Harbor agreement, the United States Department of Commerce, have been racing to complete long-running negotiations for a new agreement on transatlantic data transfers that addresses the issues raised in the Judgment. In Washington this week to lead these negotiations for the EU, Commissioner for Justice, Consumers, and Gender Equality Veøa Jourová said she is ''confident that we will meet the deadline of January 2016 for a new agreement . . . .''(14 PVLR 2043, 11/9/15)

If they succeed, a new agreement would address the Judgment by establishing a new legal basis for transatlantic data transfers. However, any such agreement will likely face legal challenges before DPAs and courts and ultimately before the CJEU again. Thus, even with a new agreement, there will still be concerns for companies that are involved in data transfers from the EU.

Background

The Judgment was issued following a referral by the Irish High Court in the case of *Schrems v Data Protection Commissioner*[3] (13 PVLR 1093, 6/23/14). The case originates from a complaint filed with the Irish DPA against Facebook Inc.'s Irish subsidiary, Facebook Ireland Ltd., in respect of concerns raised by Austrian law student Max Schrems that electronic communications transferred from Facebook Ireland Ltd. to Facebook's servers in the U.S. in reliance on EU-U.S. Safe Harbor could be accessed by the US government's National Security Agency's (**NSA**) PRISM surveillance program; a program that permits the NSA to target non-US citizens for foreign intelligence purposes. The Irish DPA rejected the complaint as unfounded on the basis that it was obligated to follow the Commission's decision in 2000 on the adequacy of data protection under the Safe Harbor Framework[4]. Mr. Schrems filed an application for judicial review in the Irish High Court. This application was granted but the case was adjourned on 18 June 2014 pending a referral to the CJEU for a preliminary ruling on the question whether the Commission's EU-U.S. Safe Harbor decision precluded a DPA from investigating complaints of inadequate levels of data protection in the US.

The CJEU Judgment

The Judgment contained two major rulings. Most significantly, as noted above, the CJEU declared the Commission's EU-US Safe Harbor decision invalid with immediate effect. In addition, the CJEU ruled that DPAs ''must be able to examine with complete independence'' whether international transfers of personal data from the EU comply with the requirements of the EU Data

Protection Directive[5] (the **Directive**), including adequacy requirements. However, the CJEU also confirmed that DPAs may not adopt measures contrary to a Commission decision of adequacy until such time as the decision is declared invalid by the CJEU and that only the CJEU has jurisdiction to make such a declaration.

Suspension of EU-U.S. Safe Harbor

The CJEU broke its analysis of invalidity of the Commission's EU-U.S. Safe Harbor decision into three parts, first analyzing the Commission's powers under Article 25 of the Directive to approve the Safe Harbor Framework. The CJEU then considered the derogation for national security in Annex 1 of the Commission's decision incorporated by Article 1 of the decision; this derogation parallels the derogation in Article 13 of the Directive. Finally, the CJEU addressed the provision in Article 3 of the Commission's decision that constrained the authority of DPAs to suspend data transfers pursuant to Safe Harbor.

In discussing the Commission's decision-making under Article 25, the CJEU reasoned that both the level of protection required for ''adequacy'' and the Commission's authority must be ''read in light of the Charter [of Fundamental Rights of the European Union][6] (the **Charter**).'' While the Charter did not become binding until the entry into force of the Treaty of Lisbon in 2009, the CJEU ruled that ''account must also be taken of the circumstances that have arisen after the decision's adoption.'' As a result, adequacy requires that the level of protection for fundamental rights must be ''essentially equivalent to that guaranteed within the European Union . . .'' and ''the Commission's discretion as to the adequacy of the level of protection ensured by a third country is reduced . . . .'' The Commission also must ''check periodically'' that the basis for adequacy remains justified.

The CJEU then applied these standards in light of the Charter to examine what the Commission's Safe Harbor decision did to ensure a level of protection equivalent to that in the EU. Although the CJEU in many respects followed the advisory Opinion of Advocate General Yves Bot, published shortly before the Judgment on 23 September 2015, it took a different tack in address-

[3] Case C-362/14, *Schrems v Data Protection Commissioner* [2014]

[4] 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and frequently asked questions issued by the U.S. Department of Commerce, OJ2000 L215/7.

[5] EU Data Protection Directive (95/46/EC)

[6] Charter of Fundamental Rights of the European Union (2000/C 364/01).

  PVLR ISSN 1538-3423

ing the claims in the case regarding U.S. government surveillance. The CJEU did not attempt to describe the US legal system relating to surveillance. The CJEU instead referred to statements in Commission reports in 2013 that suggested lack of appropriate judicial redress for EU citizens in respect of their data subject rights and broad, undifferentiated access to personal data by US authorities, and found the Commission's decision on Safe Harbor did not include findings or provisions that address these matters.

The CJEU stated, with reference to the case of *Digital Rights Ireland*[7], that in accordance with EU law ''derogations and limitations in relation to the protection of personal data [must] apply only in so far as is strictly necessary'' and this is not the case if public authorities are granted unfettered access to all personal data. The CJEU confirmed that a finding of adequacy based on a level of ''protection essentially equivalent to that guaranteed within the [EU]'' or ''guaranteed in the EU legal order'' requires an assessment of ''the content of the applicable rules in that [third] country resulting from its domestic law or international commitments and the practice designed to ensure compliance with those rules . . . .'' The benchmark of the level of protection within the EU logically calls for a similar assessment of the laws in the EU, including those relating to government surveillance by Member States.

The CJEU identified other requirements that must be addressed to establish ''essentially equivalent'' protections. These include ''administrative or judicial means of redress, enabling, in particular, the data relating to [an individual] to be accessed. . .rectified or erased'' which the CJEU considers an absence of respect for the essence of the ''fundamental right to effective judicial protection.''

Finally, with regard to Article 3 of the Commission's decision on Safe Harbor, the CJEU held that the constraints on the DPAs' independent powers under Article 25 of the Directive exceeded the Commission's power. Given the procedural context of the case, the CJEU did not consider there to be ''any need to examine the content of the Safe Harbor principles'' and carry out the essential equivalency test itself.

Building on the decision in *Digital Rights Ireland*[8], the CJEU's application of the Charter to the Commission's discretion under Article 25 of the Directive and its requirement that derogations for national security common to the Directive and other EU instruments do not obviate an obligation to ensure that certain fundamental rights are protected affects more than surveillance in the United States. The French Court of Cassation as it considers the *loi de renseignement* enacted last summer, the U.K. Parliament as it considers the recently-proposed Investigatory Powers Bill (14 PVLR 2046, 11/9/15), and other EU governments as they consider their surveillance powers in light of the wanton attacks in Paris will need to take into account the CJEU decision.

Investigatory Powers of DPAs

The Judgment on Article 3 flowed logically from its interpretation of the independent powers of DPAs. The CJEU confirmed that irrespective of a Commission decision determining the adequacy of a third country, an individual whose personal data has been or could be transferred to a third country has the right to lodge a complaint with its national DPA concerning the protection of rights and freedoms in respect of the processing of that data. The CJEU further declared that such a Commission decision ''cannot eliminate or reduce the powers expressly accorded to the national [DPA]'' including investigatory powers, powers of intervention and the power to engage in legal proceedings.

As such, a DPA is entitled to consider the validity of a Commission decision as to adequacy and in particular, whether the ''level of protection of fundamental rights and freedoms. . .is essentially equivalent to that guaranteed within the [EU] by virtue of [the] Directive read in light of the [Charter].'' However, DPAs do not have the power to declare such a Commission decision invalid. Instead an individual or DPA should challenge the decision in their national courts from where a referral should be made to the CJEU for a preliminary ruling on validity. A key question that has been raised is what this means for other Commission decisions of adequacy, for example, those made in respect of EU standard contractual clauses (**Model Contracts**) and whether these too are capable of examination by DPAs—the answer is seemingly so. What is key now is for DPAs to ensure they adopt a uniform approach to avoid inconsistencies for businesses operating in the EU.

The Reaction from the European Commission

Following the issuance of the Judgment, the Commission has indicated repeatedly that it is determined to protect transatlantic data flows and confirmed it is stepping-up ongoing talks with US authorities in particular, with a view to finalizing what has been described by Commissioner Jourová as a ''new comprehensive arrangement for the transfer of personal data with strong safeguards and legal protections.'' These negotiations commenced in 2013 following the Edward Snowden revelations in response to which the Commission decided to review the EU-U.S. Safe Harbor scheme and published a set of 13 recommendations. These included limiting use of the national security derogation under the Commission decision on EU-U.S. Safe Harbor only where ''strictly necessary or proportionate,'' and additional redress mechanisms for EU citizens whose personal data is processed in the U.S.

Significant progress on such an agreement had been made, albeit slowly, and prior to the Judgment all but one of the 13 recommendations had been agreed, the treatment of national security. The parties have since confirmed they are working hard to reach agreement with an urgency dictated by the Working Party's grace period.

It is evident that any agreement will face challenges in proceedings before DPAs to test its compliance with the standards set out by the CJEU. Some of the DPAs (as discussed further below) are likely to have different interpretations of the Judgment. The Working Party laid down a marker in its statement of Oct. 16, 2015, stating that while a Safe Harbor version 2.0 is ''urgently needed,'' the intergovernmental agreement will require

[7] Digital Rights Ireland and Others, C-293/12 and C-594/12. EU:C:2014:238, paragraphs 57 to 61

[8] Digital Rights Ireland and Others, C-293/12 and C-594/12. EU:C:2014:238, paragraphs 57 to 61

the inclusion of ''obligations on the necessary oversight of access by public authorities, on transparency, on proportionality, on redress mechanisms and on data protection rights.''

Commissioner Jourová said Nov. 16, 2015 that the Judgment ''does not require an identical organization of the U.S. legal system compared to the EU. But on data transfers, the U.S. has to offer safeguards which are globally equivalent to the ones . . . in Europe.'' The Judgment provided ''a clear definition of the requirements for an equivalent level of protection'' and it is those requirements that Jourová describes as being a ''partly political and partly technical series of negotiations.'' Jourová recently confirmed that the US has ''already committed to stronger oversight by the Department of Commerce, stronger cooperation between [DPAs] and the Federal Trade Commission'' and the parties are working to put in place an ''annual joint review mechanism that will cover all aspects of the functioning of the new framework, including the use of exemptions for law enforcement and national security grounds, and that will include the relevant authorities from both sides.'' We understand the ''crucial point'' of access by U.S. authorities is still being discussed and remains the ''biggest challenge.''

In guidance issued on Nov. 6, 2015, the Commission also confirmed that it ''will engage in a regular assessment of existing and future adequacy decisions, including through the periodic joint review of their functioning together with the competent authorities of the third country in question''. This recognizes that the CJEU's call to ''check periodically'' as well as to consider more closely the impact of derogations and third country laws on fundamental rights may carry over to existing adequacy mechanisms, both decisions as to third countries and Model Contracts. Until these are either reaffirmed or revised by the Commission or successfully challenged in a decision that reaches the CJEU, they remain in force in accordance with the Judgment.

Approach from Data Protection Authorities

While affirming the need for political solution to the uncertainty left in the wake of the Judgment and seeking to act with unity, the DPAs have also signalled their course ahead, and some have been eager to forge ahead. In addition to confirming the grace period described above, the Working Party stated that it still considers Model Contracts and Binding Corporate Rules effective solutions that companies can rely on to legitimize their international transfers of data, but also that it will analyze the impact of the Judgment on such solutions.

For the most part the approach taken by the individual DPAs has been consistent in that they have reinforced the *status quo* as established by the Working Party - in terms of a grace period and confirmation as to the validity of other data transfer solutions such as Model Contracts. However, in an extreme and somewhat rogue interpretation of the Judgment, the DPA of Schleswig-Holstein in Germany announced that Model Contracts can no longer be used to legalise transfers of personal data to the US and as such, data controllers based in Schleswig-Holstein must terminate the Model Contracts or at a minimum suspend the relevant transfer of data. The DPA further stated that those data controllers who continue to rely on Model Contracts for transfers to the US may be subject to a fine of 300,000 euros ($319,694). The DPA of Bremen also issued a statement confirming it expected an ''immediate reaction'' from data controllers to implement alternative data transfer solutions although it did not claim Model Contracts were no longer sufficient. Following these statements, on 21 October 2015 the German Conference of Data Protection Commissioners (the DPAs responsible at a federal and state level in Germany) released a position paper in which they called into question the validity of Model Contracts and Binding Corporate Rules and affirmed the ability of DPAs to examine the levels of data protection in a third country independently. The group of German DPAs declined to deem existing Model Contracts and Binding Corporate Rules insufficient despite the position of the DPA of Schleswig-Holstein, though they will not approve new applications to use these mechanisms.

What Companies Should do Now

As explicitly acknowledged by the U.K.'s Information Commissioner and indirectly by both the Working Party and the Commission in their support for a grace period, it may take businesses that previously relied on the Safe Harbor scheme time to consider and implement alternative solutions. Although companies, have until the end of January 2016 before DPAs will commence any enforcement actions and the U.S. and EU may reach a new transatlantic data transfer agreement before then, they need to be prepared.

Many companies are now inventorying their data flows and considering their choices of data transfer solution to ensure alternative mechanisms, such as Model Contracts are in place by the end of the grace period. Companies first need to determine what international transfers (both intra-group and to third party service providers) were previously made on reliance on Safe Harbor. They then need to analyze the types of data transferred and the purposes for the transfers. Based on this analysis, an assessment should be conducted as to which of the various data transfer solutions are viable and carry the least risk—each business and each category of transfer will be different and have different concerns. Businesses should prioritize their critical data transfers in the immediate short term. Only then should the longer term solutions such as Binding Corporate Rules be considered.

Given the prospect that Model Contracts and Binding Corporate Rules will undergo review and may face legal challenges, some companies are looking into ways to store data of EU data subjects within the EU to avoid the need for transfer mechanisms, at least on a contingency basis. Oracle recently announced it already does so, and Microsoft announced an agreement with Deutsche Telekom to act as a ''trustee'' for Microsoft cloud data in Germany (*see related report*). For many companies that are smaller or in other sectors, however, having data facilities in multiple countries is difficult at best.

In the interim, companies that have subscribed to the Safe Harbor principles should be mindful that their declarations remain in effect and are enforceable by the Federal Trade Commission as long as they are. The Safe Harbor principles follow the basic principles of the

   ISSN 1538-3423

Directive any new EU-U.S. data transfer agreement will build on them. Regardless of what mechanisms companies may choose ultimately, continued compliance with the Safe Harbor principles will help ensure they do not run afoul of regulatory requirements in the meantime.

While the Judgment was not widely predicted, what can be predicted with certainty going forward is a period of uncertainty during which companies and DPAs try to determine how to not only put in place a new intergovernmental agreement to address the issues raised by the Judgment and be robust against future challenges, but also to determine how to best to deal with international transfers in the interim.