Bloomberg Law

Privacy and Security Law Report®

EU-U.S. Privacy Shield

The Court of Justice for the European Union began a seismic year for data protection and cross-border data transfers by voiding the legal basis for transatlantic data transfers for the 4,400 companies reliant on U.S.-EU Safe Harbor, the authors write, the aftershocks of which will reverberate throughout 2017 and beyond.

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

BY CAMERON F. KERRY AND WILLIAM LONG

Cameron F. Kerry is senior counsel at Sidley Austin LLP in Washington and Boston. Kerry 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 is 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 U.S.-EU Safe Harbor Decision (the Judgment) is a landmark judgment. Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650. By voiding the legal basis for transatlantic data transfers for the 4,400 companies reliant on U.S.-EU Safe Harbor, the Judgment began what has been a seismic year for data protection and cross-border data transfers[1] in the European Union, whose aftershocks will reverberate throughout 2017 and beyond.

The U.S. and EU moved quickly to put in place a new, reinforced data transfer framework in U.S.-EU Privacy Shield that responds to issues in the Judgment, and which was formally adopted by a European Commission adequacy decision on July 12, 2016. Nevertheless, the grounds of the Judgment invited challenges to the

[1] 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

Privacy Shield and raised doubts about other existing data transfer mechanisms that could reshape the way in which data is transferred across the Atlantic and globally. Further, by empowering data protection authorities to review adequacy decisions independently of the European Commission, the Judgement has expanded avenues to challenge these mechanisms. At the same time, the passage of the EU's General Data Protection Regulation (GDPR) in May 2016 is requiring companies and DPAs with a great deal of preparation and many questions to answer by May 25, 2018. The only certain thing that one can say is that vast uncertainty is a feature of the EU privacy and data protection landscape in 2017 and, perhaps beyond.

Background

The Judgment was issued following a referral by the Irish High Court in the case of *Maximilliam Schrems v Data Protection Commissioner*. 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 U.S.-EU Safe Harbor could be accessed by the U.S. government's National Security Agency's (NSA) PRISM surveillance program; a program that permits the NSA to target non-U.S. 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. Mr. Schrems filed an application for judicial review in the Irish High Court. This application was granted but the case was adjourned on June 18, 2014 pending a referral to the CJEU for a preliminary ruling on the question whether the Commission's U.S.-EU Safe Harbor decision precluded a DPA from investigating complaints of inadequate levels of data protection in the U.S.

The only certain thing is that vast uncertainty is a feature of the European Union privacy and data protection landscape in 2017 and, perhaps beyond.

The CJEU Judgment

The Judgment contained two major rulings. Most significantly, the CJEU declared the Commission's U.S.-EU 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 (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 U.S.-EU Safe Harbor

The CJEU broke its analysis of invalidity of the Commission's U.S.-EU 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'' (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 Sept. 23, 2015, it took a different tack in addressing the claims in the case regarding U.S. government surveillance. The CJEU did not attempt to describe the U.S. 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 U.S. authorities. It also 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 and Others*, 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.

  PVLR ISSN 1538-3423

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 and Others*, 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. A number of EU governments (including those in France and the U.K.) have had to consider their surveillance provisions in light of the recent attacks in Belgium, Paris and Germany. Although, at least from a U.K. perspective, the recently adopted Investigatory Powers Act 2016, referred to by privacy advocates as the ''Snoopers Charter'' will likely be subject to further review prior to entering into force as a result of the CJEU's recent ruling in *Tele2 Sverige AB*, which states that the ''general and discriminate'' way in which the U.K. government was retaining data for the purposes of criminal investigations was incompatible with EU law and indicates that the CJEU has an expansive view of its competence in the domain of national security and law enforcement. *Tele2 Sverige AB v. Post-och telestyrelsen* C-203/15, and *Secretary of State for Home Department v. Tom Watson and Others* C-698/15.

The Birth of the EU-U.S. Privacy Shield

Immediately following the issuance of the Judgment, the Commission stepped up ongoing talks with U.S. authorities to conclude a new framework on transatlantic data flows. Accordingly on Feb. 2, 2016, the Commission announced that a political agreement had been reached on the new framework now known as the EU-U.S. Privacy Shield and the draft documentation was published on Feb. 29, 2016.

According to the Commission, the EU-U.S. Privacy Shield is designed to ''[protect] the fundamental rights of Europeans and [ensure] legal certainty for businesses, including European companies, transferring personal data to the U.S.'' The framework expands on the principles set out in the Safe Harbor Framework and purports to address the concerns highlighted by the Judgement including in respect of onward transfers, redress mechanisms and the individual rights of data subjects.

As was the case under the Safe Harbor Framework, companies participating in the EU-U.S. Privacy Shield need to certify compliance with a number of Principles and Supplemental Principles. Although the Privacy Shield Principles are incorporated, some have been substantially rewritten, for example, the Accountability for Onward Transfer Principle includes a requirement to notify where a third-party recipient is unable to provide the same level of protection as is required under the Privacy Shield Principles. This is intended to ensure that requirements cannot be circumvented by transferring processing to a third party and that additional assurances in the Privacy Shield regarding access to data by government authorities remain in place where onward transfers take place.

The Article 29 Working Party (the Working Party) published an opinion on the draft documentation on April 13, 2016 (the WP29 Opinion). The WP29 Opinion acknowledged a number of significant improvements as compared to the Safe Harbor Framework with regards to commercial privacy issues but raised concerns including that the data retention principle was not explicitly referenced and that the redress mechanisms were too complex. With regard to access by public authorities, the Working Party expressed concerns regarding the independence of the ombudsperson and its lack of adequate powers to provide satisfactory remedy and the scope of a U.S. Government reservation for bulk surveillance in certain circumstances.

The European Parliament and the European Data Protection Supervisor both issued similar opinions. Both bodies saw a need for a more ''user-friendly'' redress system and for clarification on the written assurances by the U.S. regarding bulk data collection. Following the reviews, the EU and U.S. officials recommenced negotiations to finalise the documentation, attempting to address the concerns of the relevant stakeholders.

To date there are over 1,500 self-certified companies on the EU-U.S. Privacy Shield List.

The revised Privacy Shield text was sent to the Article 31 Committee for their review and received approval on July 8, 2016. The adequacy decision establishing that the U.S. ensures an adequate level of protection for personal data transferred under the EU-U.S. Privacy Shield from the EU to participating companies in the U.S. was adopted by the Commission on July 12, 2016. From Aug. 1, 2016 companies in the U.S. have been able to self-certify under the Privacy Shield Framework and to date there are over one thousand self-certified companies on the Privacy Shield List.

The key documentation for the Privacy Shield Framework includes:

(i) the Privacy Principles and Supplemental Principles;

(ii) commitments from the heads of the U.S. Department of Commerce, Department of Transportation, Department of State, and Federal Trade Commission (FTC) with regard to enforcement and implementation of the framework; and

(iii) letters from the Office of the Director of National Intelligence (ODNI) and the U.S. Department of Justice to the U.S. Department of Commerce that describe the limitations and safeguards applicable to U.S. government access.

According to the Commission and the Department of Commerce, the Privacy Shield used the CJEU ruling as a ''benchmark'' to include a number of new elements and materially more stringent and detailed provisions as compared to the Safe Harbour Framework, including:

■ **Ombudsperson**—the Under Secretary of State for Economic Growth, Energy, and the Environment serves as the independent Privacy Shield Ombudsperson with respect to individual complaints regarding possible access by national intelligence authorities. This Under Secretary is also the official vested with presidential authority under President Obama's Presidential Policy Directive 28 to ''coordinate'' diplomacy on international information technology issues and ''to serve as a point of contact for foreign governments who wish to raise concerns regarding [U.S.] signals intelligence activities . . .'' The U.S. government has taken steps to assure the independence of the Ombudsperson via an inter-agency process to review complaints made to the Ombudsperson, filtered through Member State bodies with oversight of national security services. The role of the Privacy Shield Ombudsperson extends beyond the Privacy Shield to encompass complaints relating to other international data transfer frameworks including the proposed EU General Data Protection Regulation (GDPR).

■ **Annual Joint Review and Enhanced Enforcement**—an annual joint review will be conducted by the Commission and the U.S. Department of Commerce, assisted by U.S. security and intelligence agencies, the Ombudsperson, and DPAs to look at all aspects of the Framework, including access by public authorities. The Commission also retains the right to suspend the adequacy decisions of the Privacy Shield Framework if the commitments are not met by the U.S.

■ **Access by U.S. Government**—the U.S. government (through the ODNI) has provided written assurances that access to personal data by U.S. public authorities for law enforcement, national security and other public interest purposes will be subject to specific articulated limitations, safeguards, and oversight mechanisms (such as the Ombudsperson mechanism) that safeguard against generalized access. The U.S. further assures that there is no indiscriminate or mass surveillance on the personal data transferred to the U.S. under the Privacy Shield.

■ **Avenues of Redress for EU Individuals**—the framework provides a menu of redress options for data subjects. In the first instance, individuals can complain to the U.S. participating company. The company will have to respond to the complaint within 45 days. To the extent U.S. companies are handling human resources data of EU individuals, they will also need to commit to comply with decisions from European DPAs. Other companies may voluntarily commit to submitting complaints to a panel of DPAs. An unresolved complaint can then be dealt with through an alternative dispute resolution procedure, in which all U.S. participating companies must take part, and which will be at no cost to the individual. An EU individual or a DPA can also refer a still-unresolved complaint to a specified team at the U.S. Department of Commerce, which must respond within 90 days, or to the FTC where the Department of Commerce is unable to resolve the matter. In addition, where DPAs have jurisdiction over the transferring company, they can take action. As a last resort, where a DPA does not have jurisdiction, individuals can refer complaints to a binding arbitration panel, the Privacy Shield Panel, which would ensure a binding and enforceable decision subject to judicial enforcement under the U.S. Federal Arbitration Act.

Challenges to Data Transfer Mechanisms

Following the adoption of the EU-U.S. Privacy Shield, the Working Party chairman, Isabelle Falque-Pierrotin, announced that EU DPAs would not launch legal action of their own initiative but would wait until after the first annual review. In assessing the impact of this statement, it must be noted that neither the Working Party nor its members (the DPAs) can launch direct legal action against the Privacy Shield. Only Member States and EU Institutions (such as the European Parliament) can submit such challenges. DPAs can only ask a national court, in the context of a pending dispute, to refer a question on the validity of the Commission's Privacy Shield Decision to the CJEU.

This one-year hiatus has not prevented others from challenging the validity of both the EU-U.S. Privacy Shield Framework and of other cross-border data transfer mechanisms.

Only Member States and European Union Institutions—not the Article 29 Working Party or national privacy regulators—can launch direct legal action against the EU-U.S. Privacy Shield.

Following its disposition by the CJEU, Max Schrems' case went back to the Irish High Court, and from there to the Irish Data Protection Commissioner (IDPC), where Schrems added claims relating to Facebook's transfer of data pursuant to Model Contracts. His complaint alleged that Model Contracts suffer from the same defects as the Safe Harbor Framework (i.e. deficiencies in the remedies granted to EU citizens whose data is transferred to the U.S.). In turn, on May 31, 2016, the IDPC issued court proceedings in the Irish High Court to examine the validity of the Model Contracts. The Irish High Court in turn will have to consider whether it is competent to decide the issue or whether it should refer the question to the CJEU. The High Court commenced court proceedings Feb. 7.

In addition, two legal challenges have been filed at the General Court of the CJEU challenging the Commission's adequacy decision on the EU-U.S. Privacy Shield. Individuals and or organizations may challenge EU legislation before the CJEU only if they are ''directly concerned'' by the legislation, within two months of the legislation coming into force. Digital Rights Ireland, the very same advocacy group referred to in the Judgment, was the first to bring action in the General Court of the CJEU on Sept. 16, 2016, followed by another challenge on Nov. 2, 2016 by French advocacy group La Quadrature du Net. Whether the Privacy Shield is of direct concern to either Digital Rights Ireland or La Quadrature du Net is currently under review, but if the CJEU finds

  PVLR ISSN 1538-3423

this not to be the case then the relevant action will be declared inadmissible. If deemed admissible, then it will likely take over a year before the CJEU rules on the case.

If any these cases are heard, the CJEU will be presented with a very different view than it was in the original *Schrems* case, which was decided on the basis of the allegations in Schrems's complaint (in turn based on news stories about the Edward Snowden disclosures). This time, Facebook is appearing in the Irish case, where the U.S. government and a variety of trade associations and civil society organizations have been granted intervention. At least 12 parties including the Commission and U.S. government have requested intervention in the Digital Rights Ireland case; responses have not been filed yet in la Quadrature du Net's case.

Adding to the uncertainly about transatlantic data transfers are questions about what the new U.S. administration will do with regard to international agreements and foreign surveillance that could affect the Privacy Shield. To date, President Trump has not taken any actions to undo Presidential Policy Directive 28 and the safeguards that underlie the European Commission's July 25 adequacy decision. Headlines concerning a provision in a Jan. 25 executive order on immigration suggested that might not be the case, but in fact the provision does not affect either surveillance reforms and the Commission issued a statement confirming it does not affect the Privacy Shield. Nevertheless, there is clearly anxiety in the EU and elsewhere that the new administration might take actions that could cause the Commission to consider suspending the Privacy Shield framework by the time of the first annual review in mid-2017 or provide ammunition for legal challenges.

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.

The Judgment arguably opened the flood gates for DPAs to question the legal validity of other Commission decisions of adequacy, for example, those made in respect of EU standard contractual clauses (Model Contracts) which are standard form data transfer agreements between a data exporter in the EU and a data importer outside the EU.

It remains to be seen whether particular DPAs, such as those in Germany, will be more willing to prohibit or suspend international data flows under the Model Contracts Decisions. On Oct 21, 2015, following the Judgement, 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 did not approve new applications to use these mechanisms. Moreover, the relevance that these decisions may have on the ongoing litigation in Ireland remains an open question.

In the meanwhile, the Commission adopted two Implementing Decisions (the Model Contract Decisions) as a consequence of the Judgement which would amend the existing adequacy decisions that underpin the Model Contracts for the international transfer of personal data, in particular, amending the power of the DPAs. The Model Contracts Decisions sought to uphold the Judgement to declare that DPAs remain competent to oversee the transfer of personal data to a third country which has been the subject of a Commission adequacy decision and that the Commission has no competence to restrict their powers under Article 28 of the Directive. The Model Contracts Decisions thus stated ''in the light of the [Judgment] and pursuant to Article 266 of the Treaty, the provisions in those Decisions limiting the powers of the national supervisory authorities should therefore be replaced.''

Adding to the uncertainly about transatlantic data transfers are questions about what the new U.S. administration will do with regard to international agreements and foreign surveillance.

The Commission has also indicated that it intends to undertake a review of the existing adequacy decision for ten countries other than the United States, recognising that most of the defects the CJEU identified in the Judgment apply to these decisions. This is particularly the case with respect to countries found adequate that also engage in intelligence collection—Argentina, Canada, Israel, and New Zealand (unlike, say, Andorra or the Isle of Man so far as anyone knows).

What Companies Should Do Now

The Commerce Department has reported that some 1,565 companies have subscribed to the Privacy Shield. Many of these are companies that took advantage of the nine-month grace period for reforming contract provisions by subscribing before October, and some are consumer-facing companies for which Model Contracts are a sub-optimal solution and for which the Privacy Shield offers a form of ''trust mark'' they can offer to customers in Europe.

Now that there is less immediacy, companies that are taking steps to comply with the GDPR may wish to consider combining preparation for the Privacy Shield, which requires some of the same steps. For example:

Data Mapping: in order to determine the types of personal data collected, the purposes for which this is processed and who the recipients of the personal data are (including in respect of international transfers), a form of data mapping exercise should be carried out. The report generated would not only assist in completing a Privacy Shield application but also satisfy the requirement under the GDPR for businesses to maintain a detailed record of their data processing activities.

Notice and Consent: the GDPR introduces new requirements as to the information that should be provided in notices, as well as new consent requirements. Companies can combine their review of existing employee and customer data privacy notices, consents and policies with their review of the same from a Privacy Shield perspective.

Companies that are taking steps to comply with the European Union General Data Protection Regulation may wish to consider combining preparation for the Privacy Shield.

Individual Rights: both the GDPR and the Privacy Shield place great emphasis on data subject rights with, for example, the introduction of an individual's right to have their personal data erased, in certain circumstances and a new right to data portability under the GDPR. Businesses should consider how in practice they will implement the various privacy rights and in particular, the right to erasure which may involve a review of existing data retention policies and procedures.

Information Security: as with the GDPR, the security obligations under the Privacy Shield have been drafted deliberately vague as the level of security required will depend on the activities of the business and the types and volumes of personal data processed. In addition, under the GDPR, business will be subject to security breach reporting obligations, something many US companies are already familiar with. In readiness, businesses should be reviewing and updating existing information security standards and policies. Businesses should also consider implementing a vendor management program. This would typically address the following: (i) due diligence during the vendor selection process to assess from a data privacy perspective the internal controls and operations of the vendor; (ii) the implementation of appropriate data processing agreements; (iii) the development and implementation of a minimum set of vendor security requirements; and (iv) the carrying out of vendor audits throughout the term of the agreement. This is particularly important as it will assist with the onward transfer requirements under the Privacy Shield and the data processing obligations under the GDPR.

Vendor Contracts and Onward Transfers: from a GDPR perspective, contracts with any service providers involved with the processing of EU personal data should be reviewed (or implemented) to ensure the appropriate data processing and liability wording is in the contract as well as specific timeframes for reporting security breaches. When reviewing these contracts and to the extent necessary, the provisions required in order to comply with the Onward Transfer Principle under the Privacy Shield could also be inserted.

  PVLR ISSN 1538-3423