The demise of the US-EU Safe Harbor

Bridget Treacy, Partner, and James Henderson, Associate, Hunton & Williams, examine the uncertain position left by the CJEU after it declared Safe Harbor invalid

On 6th October 2015, the Court of Justice of the European Union ('CJEU') gave its judgment in the case of *Max Schrems v Data Protection Commissioner of Ireland* (Case C-362/14). As has been widely reported, the CJEU declared the US-EU Safe Harbor, a mechanism that has facilitated the transfer of personal data between the EU and the US for 15 years, to be invalid. It also found that national Data Protection Authorities ('DPAs') are not absolutely bound by adequacy decisions of the European Commission, and may conduct their own investigations into whether transfers of personal data are subject to an adequate level of protection.

The decision has attracted lurid media headlines and has created a sense of panic in some quarters. Organisations are now scrambling to implement alternative data transfer mechanisms ahead of anticipated DPA enforcement actions.

The facts

In the wake of Edward Snowden's revelations about the widespread access to personal data enjoyed by US intelligence agencies, Mr Schrems, an Austrian privacy campaigner, made a complaint to the Irish DPA, challenging Facebook's use of Safe Harbor to transfer personal data to the US.

Mr Schrems alleged that the Safe Harbor did not provide an adequate level of protection for EU personal data in the US. He asked the Irish DPA to examine its validity and, if necessary, to suspend ongoing transfers of personal data to the US by Facebook.

Origins of Safe Harbor

The Safe Harbor framework was developed to address European concerns that data privacy protections in the US were not 'adequate', as required by Article 25(1) of the EU Data Protection Directive ('Directive'). The framework was negotiated by the US Department of Commerce and the European Commission to bridge the different privacy approaches in the US and Europe, and to provide a streamlined means for EU organisations to transfer personal data from Europe in compliance with the Directive.

Until the CJEU's judgment in Schrems, organisations that self-certified to the Safe Harbor framework were legally permitted to receive personal data originating from Europe. The framework itself comprised a set of Privacy Principles and Frequently Asked Questions. To certify to the Safe Harbor, organisations: (1) conformed their privacy practices to meet the requirements of the Safe Harbor Privacy Principles; (2) filed a self-certification form with the Department of Commerce; and (3) published a Safe Harbor privacy policy, stating how the company complied with the Privacy Principles.

EU criticism of Safe Harbor

EU criticism of Safe Harbor is nothing new, but it intensified following Edward Snowden's disclosures in June 2013.

Prior to that, in April 2010, the Düsseldorfer Kreis (a working group comprised of the 16 German state DPAs responsible for the private sector), issued a resolution requiring additional diligence on the part of German data exporters transferring data to Safe Harbor certified entities. By requiring additional diligence, the German DPAs appeared to question the European Commission's decision that Safe Harbor certification is sufficient to demonstrate an adequate level of protection for personal data.

In July 2012, the Article 29 Working Party adopted an opinion on cloud computing in which it similarly concluded that EU data exporters could not rely on self-certification alone. The Working Party noted that in order to legitimise data transfers to cloud vendors located in the US, data exporters may need to obtain evidence of compliance with the Safe Harbor framework.

Following the Snowden revelations, the rumblings of discontent with Safe Harbor crystallised when the European Parliament called on the European Commission to review Safe Harbor, claiming that the PRISM programme and access to personal data originating from the EU by US law enforcement

(Continued on page 4)

(Continued from page 3)

agencies constituted a 'serious violation' of the Safe Harbor Agreement.

Mr Schrems' claim

Mr Schrems' complaint was made against the backdrop of this growing European discontent with Safe Harbor. He did not attack the Safe Harbor principles directly, but attacked the activities of US law enforcement and intelligence agencies and their access to and use of EU personal data in the US.

Schrems' central claim was that the Safe Harbor no longer provided an adequate level of protection for personal data, because of US agencies' blanket access to data, as revealed by Edward Snowden. Mr Schrems requested that the Irish DPA order Facebook to suspend data transfers to the US under Safe Harbor.

The specific question referred to the CJEU by the Irish High Court was whether the Irish DPA was bound by the Commission's adequacy decision on Safe Harbor, precluding any investigation by the DPA into the protection afforded to data transferred in those particular circumstances, or whether the DPA could conduct its own investigation into the ongoing adequacy of the Safe Harbor, in light of the factual developments since the Commission's adequacy decision (Decision 2000/520).

CJEU's judgment

The CJEU found that national DPAs are not bound by Commission adequacy decisions, but are entitled to conduct their own investigation into whether transfers of personal data are subject to an adequate level of protection. In addition, the Court went further than the specific question referred to it, and considered whether Decision 2000/520 on which the Safe Harbor rests is valid. The CJEU decided that it is not.

"In the immediate aftermath of the judgment, a number of affected companies have already started to implement alternative data transfer mechanisms. Some vendors have proactively sent pre-executed Model Clauses to EU clients."

Meaning of 'adequate'

In considering the validity of Decision 2000/520, the Court noted that the requirement of 'adequacy' does not mean that a third country must ensure a level of protection for personal data that is 'identical' to that guaranteed in Europe. Rather, the level of protection for fundamental rights and freedoms must be 'essentially equivalent' to those guaranteed in Europe. This is a question of fact that requires consideration of domestic law and a country's international commitments. Further, as the level of protection may change, the court considered that the Commission would need to 'check periodically' whether the adequacy finding remained 'factually and legally justified'.

Surveillance by US law enforcement

Decision 2000/520 provides that national security and law enforcement considerations have primacy over the Safe Harbor Principles. The court found that this general derogation enabled interference with the fundamental rights of European citizens, without limit or effective legal protection. In other words, although organisations might certify to, and in fact comply with, the Safe Harbor Principles, access on a generalised basis by US law enforcement and intelligence agencies would mean that EU citizens' personal data are not adequately protected.

Prior to publication of the judgment, the US trade mission to the EU was quick to rebut assumptions concerning Snowden that had appeared in the Advocate General's Opinion, stating that "[t]he United States does not and has not engaged in indiscriminate surveillance of anyone, including ordinary European citizens", and that the PRISM programme "is in fact targeted against particular valid foreign intelligence targets, is duly authorized by law, and strictly complies with a number of publicly disclosed controls and limitations."

Absence of right of redress for EU citizens in US

Another important factor for the CJEU was that EU citizens have no right of redress in the US in relation to the use of their data by such agencies.

In the EU, the right of redress to an independent authority is a fundamental right and essential to ensure that individuals are protected. Although the Federal Trade Commission in the US is responsible for ensuring that companies do not engage in unfair or deceptive trade practices (including misrepresentation as to their compliance with the Safe Harbor), its jurisdiction does not extend to use of data by law enforcement agencies. Consequently, the CJEU was of the view that the Safe Harbor does not provide an adequate level of protection for personal data.

It should be noted that the CJEU did not engage in any direct comparison between the use of data by US law enforcement and intelligence agencies, and those in the EU. Edward Snowden's revelations revealed similar surveillance activities carried out by EU-based intelligence agencies, particularly those in the UK.

The use of personal data in the EU for the purposes of law enforcement and the protection of national security is not subject to the Data Protection Directive, and arguably the use of data by EU-based intelligence agen-

cies is subject to no greater level of supervision or proportionality to that of US-based intelligence agencies, a point noted by several commentators. EU citizens may, however, bring court action in their jurisdiction to object to the use of their data for such purposes, but are not currently afforded equivalent rights in the US.

Implications for business

The CJEU's decision has created significant uncertainty for business. Whilst the suspension of the Safe Harbor is of immediate concern for the 4,000 companies that currently hold a Safe Harbor certification, it also raises the prospect of disruption for the many thousands of EU affiliates and customers that rely on the Safe Harbor certifications of those companies.

The CJEU judgment has created a vacuum and significant uncertainty for all organisations that rely on the Safe Harbor.

National DPAs may investigate transfers

Some of the present uncertainty stems from the CJEU's ruling that national DPAs must investigate the adequacy of protection afforded to transfers of personal data outside of the EU where data subjects lodge complaints.

Prior to the Schrems case, organisations were afforded a degree of certainty in relation to reliance on the Safe Harbor and other adequacy decisions. Following Schrems, organisations may need to contend with different approaches adopted in individual Member States or, in a worst case scenario, different approaches adopted on a case by case basis.

The Article 29 Working Party is discussing these issues and is expected to issue guidance in the coming days.

The European Commission has also announced its intention to publish guidance. It is crucial that any such guidance adopts a coordinated approach, providing consistency for organisations that previously relied on the Safe Harbor. In the absence of this, organisations will need to consider their data transfer strategy on a country-by-country or even case-by-case basis.

Validity of other transfer mechanisms questioned

A further source of uncertainty concerns the validity of other available data transfer mechanisms, such as Model Clauses.

At the heart of the Schrems case is the fact that US law enforcement and intelligence agencies have the ability to access EU personal data once they are held in the US. The access rights of US law enforcement and intelligence agencies to data transferred to the US are not specific to data transferred under the Safe Harbor, but apply to data transferred under other mechanisms, such as the EU Model Clauses. It remains to be seen whether other data transfer mechanisms will be challenged but, for now, Model Clauses and the other mechanisms remain valid.

The Court gave some reassurance in relation to the validity of other data transfer mechanisms. While recognising that national DPAs are required to investigate complaints, the Court explicitly reserved to itself the power to invalidate other adequacy decisions. These decisions could be subject to challenge, but this would require a referral of the case to the CJEU and a finding by the court that the adequacy decision was invalid. The result is that, at least in the short term, the other available transfer mechanisms remain valid.

Immediate next steps

In the immediate aftermath of the judgment, a number of affected companies have already started to implement alternative data transfer mechanisms. Some vendors have proactively sent pre-executed Model Clauses to EU clients.

Before doing anything, businesses should first assess the nature and extent of their EU-US data flows, and the extent to which they may be covered by other data transfer mechanisms or the derogations available under the Directive. Appropriate solutions will depend on the nature and extent of a company's EU-US cross border data flows. Apparently simple alternatives to Safe Harbor, such as Model Clauses, require careful planning, not least to ensure that the clauses will cover the correct data flows, and are executed by the correct entities. Approximately half of the EU Member States require Model Clauses to be filed with the DPA or approved by them, and DPA registrations may need to be updated.

Some organisations are turning to Binding Corporate Rules. These offer a good solution but are a longer term project.

In the UK, the Information Commissioner's Office ('ICO') has indicated that it might allow organisations an initial grace period. The Article 29 Working Party has also issued a statement, saying that pending a long term solution, BCRs and Model Clauses may be used to legitimize EU/US data transfers. The Working Party urged for that solution to be in place by January 2016.

Future of the US-EU Safe Harbor framework?

Negotiations to improve the US-EU Safe Harbor Framework between the European Commission and the US Department of Commerce are ongoing. 'Safe Harbor 2.0' has not yet been agreed. Despite calls for a formal statement on the revised regime, Safe Harbor 2.0 remains in limbo, and it remains to be seen whether it is now a realistic prospect at all. While the original Safe Harbor may have been consigned to history, the future without it currently looks uncertain.

Bridget Treacy and James Henderson
Hunton & Williams
btreacy@hunton.com
jhenderson@hunton.com