The fall of Safe Harbour and the future of transatlantic data sharing

The basis of Safe Harbour has been questioned for some time, and in recent years it has become increasingly apparent that an updated privacy regime is necessary, Natasha Simmons writes.
Introduction
On 6 October 2015, the Court of Justice of the European Union (CJEU) delivered its landmark judgment on Safe Harbour in the case of Maximilian Schrems v Data Protection Commissioner [Case C-362/14]. The CJEU ruled that Commission Decision 2000/520/EC concerning transfers of personal data to US companies, and establishing the ‘adequacy’ of the Safe Harbour certification system, is in fact invalid. The decision reflects what many in Europe consider, that present laws are outdated, and the law must adapt to catch up with the pervasiveness of technology in the digital age.

“Legal rules that were written at the dawn of the personal computer are no longer adequate for an era with ubiquitous mobile devices connected to the cloud.”

Background
In the aftermath of Edward Snowden’s revelations about US intelligence agencies’ extensive access to personal data, Austrian privacy campaigner, Max Schrems, made a complaint to the Irish Data Protection Authority (DPA), challenging Facebook’s reliance on Safe Harbour for personal data transfers from the EU to the US. Schrems claimed that the Safe Harbour program did not ensure an adequate level of protection for EU personal data being transferred to the US. Schrems also requested that the Irish DPA examine the validity of Safe Harbour, and, if required, that the Irish DPA suspend Facebook’s transfers of personal data to the US.

The Safe Harbour framework
Under the Data Protection Directive (95/46/EC), the transfer of personal data to a third country, in principle, may only take place if the third country ensures an adequate level of protection of the personal data. The Commission may make a finding that a third country provides an adequate level of protection due to its domestic law or international commitments. Commission Decision 2000/520/EC on Safe Harbour was an example of this. Prior to the ruling
of the CJEU in the *Schrems* case, organisations signed up to self-certification under the Safe Harbour framework could legally receive personal data being transferred from Europe.

The framework included a set of privacy principles and frequently asked questions. In order to be certified under Safe Harbour, organisations had to ensure that their privacy practices met the requirements of the Safe Harbour Privacy Principles. They also had to file a self-certification form with the Department of Commerce, and, in addition, publish a Safe Harbour privacy policy setting out how the company ensured compliance with the principles.

**The decision**

In its judgment, the CJEU considered the roles of the European Commission, and the national supervisory authorities, as well as the fundamental rights enshrined in European law. The CJEU held that the existence of a Commission decision finding that a third country ensures an adequate level of protection of personal data transferred cannot

It appears that we are about to witness the construction of a new framework, and we must be prepared for the wave of change approaching
remove, or reduce, the powers available to the national supervisory authorities under the Charter of Fundamental Rights of the European Union and the data protection directive (95/46/EC). The Court emphasised the right, guaranteed by the Charter, to the protection of personal data and the role with which the national supervisory authorities are entrusted thereunder. The Court stated that no provision of the directive prevents oversight by the national supervisory authorities of transfers of personal data to third countries which have been the subject of a Commission decision.

The Court noted that the national supervisory authorities must be able to examine, with complete independence, whether the transfer of a person’s data to a third country complies with the requirements laid down by the directive. Nevertheless, the Court pointed out that it alone has jurisdiction to declare that an EU act, such as a Commission decision, is invalid. An individual or national supervisory authority must be able to bring proceedings before the national courts so that they may refer the case to the Court of Justice.

The CJEU then investigated whether the Safe Harbour decision is invalid. In this respect, the Court stated that the Commission was required to find that the United States in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed within the EU under the directive, read in the light of the Charter. The Court noted that the Commission did not make such a finding, but merely examined the Safe Harbour program. For those reasons, the Court declared the Safe Harbour Decision invalid.

The result of the ruling is that the Irish supervisory authority is required to examine Schrems’ complaint and, following its investigation, is to decide whether, with regard to the directive, transfer of the data of Facebook’s European subscribers to the US should be suspended on the ground that that country does not afford an adequate level of protection of personal data.
Response from regulators
The Article 29 Working Party (WP), comprised of EU national data protection authorities, met shortly after the Schrems ruling with the aim of adopting a harmonised approach to the decision, and avoiding a varied response throughout member states. The WP released a statement thereafter, on 16 October 2015, which addressed the case and its wider implications. The WP commented that the matter of massive and indiscriminate surveillance was a key element of the CJEU’s reasoning.

The WP also granted a three month grace period, indicating that the EU and the US will have until the end of January 2016 to find a political, technical, or legal solution to this matter. The EU Commission issued guidance, on 6 November 2015, with the objective of ensuring a consistent response from national regulators and offer legal certainty for businesses. The Commission indicated that it remains committed to the goal of a renewed and sound framework for transatlantic personal data transfers. The Commission also advised that companies may use a number of alternative tools for carrying out their international data transfers to third countries that are not deemed to grant an adequate level of protection. Further responses are anticipated at EU and national level over the coming months, and progress should be closely monitored.

With regard to the future of data transfers across the pond, it should be noted that the EU and the US have been negotiating a new Safe Harbour framework since 2013. Whilst significant progress has been made in terms of a successor program, national security derogations are still an obstacle, and there is no concrete timeframe as yet. Therefore, it is not clear when exactly a new framework will be agreed. As a result, businesses relying on a Safe Harbour 2.0 being finalised should be aware that this is not a fail-safe solution, and they risk losing consumer trust and possible enforcement action if a successor is not agreed by the end of the grace period in January 2016.
Next steps
In light of the WP’s statement, it is clear that businesses should begin evaluating the range of available alternatives in order to devise a plan of action. Notwithstanding this, companies should remain calm and avoid making rash decisions until they have carefully assessed their priorities and the alternatives available to them. It is important for organisations to be pro-active in order to demonstrate to the regulators that any necessary remediation steps have been taken to address the implications of the decision. Businesses, therefore, are advised to take steps in the aftermath of the Schrems ruling in order to determine whether they must take any compliance action.

Such an assessment should include the mapping of EU-US data flows where Safe Harbour is currently the model of transfer used, as well as identifying key elements including types of data and the purpose of transfers. Companies should focus on key data flows depending on their business operations and needs. Businesses should also consider alternative data transfer methods and select the best option for their particular organisation. In addition, organisations should assess whether any local requirements must be fulfilled, for example, regulatory filing or authorisation. It would also be useful to record the assessment and compliance steps taken, and businesses should keep up-to-date with any developments regarding Safe Harbour.

Alternative data transfer options for businesses
Whilst the CJEU ruling has a huge impact on EU-US data transfers, it should be remembered that Safe Harbour is not the only mechanism for such data transfers, and that alternatives exist. US companies that rely on the Safe Harbour framework to transfer personal data to the US will now have to consider other methods of transfer in order to comply with EU law. The ruling will affect both US processors and controllers. In addition, EU companies currently using a US Safe Harbour certified service provider will also have to consider their response to the Schrems decision. Alternative options available for data transfers from the EU to the US include EU model clauses, Binding Corporate Rules and EU data centres, among others.
In relation to the use of EU model controller-to-processor clauses, these may be used in order to comply with standards throughout all EU member states, and help to address any customer concerns regarding appropriate data protection compliance. The model clauses, however, do entail specific obligations, and may involve some administrative burden for the company. In terms of companies managing intra-group personal data transfers, one option which they may wish to pursue is that of Binding Corporate Rules (BCRs).

BCRs, however, may not always be the most suitable option as they are most appropriate in the case of intra-group transfers and for larger organisations. BCRs would be most relevant for organisations wishing to establish a global privacy compliance framework, and may not be a viable option for smaller businesses due to the time and cost constraints involved. Businesses should take the time to consider the best solution for them in light of the advantages and disadvantages of the various transfer options.

Wider considerations
The Schrems ruling raises broader considerations concerning the right to privacy, and the future of transatlantic personal data transfers in the tech age. It is difficult to envisage how privacy rights can last if their strength varies depending on when and where user data is transferred to- the fundamental right of privacy should not be impinged by overseas data transfers. This logic is present in the Schrems ruling, and other recent CJEU case law. There has been an increasing move within Europe towards reinforcing the right to privacy, which is reinforced by the draft General Data Protection Regulation (GDPR) currently making its way through the legislative process, as well as the Digital Single Market agenda.

There is a delicate and intricate balance which must be struck between protecting the fundamental human right of privacy, allowing the internet to have global reach and supporting advancing technology, whilst developing the law so that it may try to address the challenges presented by the digital world.
Conclusion
Privacy advocates who wish to see a stronger transatlantic data protection regime will likely welcome the Schrems judgment as a step in the right direction. Critics of the ruling, however, may argue that it could have a detrimental effect on smaller European businesses, who may struggle to trade with US businesses, particularly in terms of the cloud computing market.³

It is yet to be seen what the exact outcome of this ruling will be in terms of future data exchanges between the EU and US. What is clear is that this is an issue at the forefront of the privacy arena, and one to be closely watched. It influences a number of wider issues, such as internet balkanisation and the relationship between the US and Europe concerning privacy rights in the face of emerging technology. The basis of Safe Harbour has been questioned for some time, and in recent years it has become increasingly apparent that an updated privacy regime is necessary. It appears that we are about to witness the construction of a new framework, and we must be prepared for the wave of change approaching.

Natasha Simmons is an associate in the Commercial IP/IT Group at Bristows LLP

Endnotes