Briefing

November 2015

SHEPHERD+WEDDERBURN

Safe Harbour, Safe No More



Guy Harvey
guy.harvey@shepwedd.co.uk
Gordon Moir
gordon.moir@shepwedd.co.uk
Nicola Rinaldi
nicola.rinaldi@shepwedd.co.uk

On 6 October 2015 the European Court of Justice ("ECJ") ruled that the long-standing Safe Harbour arrangement between the EU and the US does not provide an adequate level of protection for European personal data (the Safe Harbour Decision).

The Safe Harbour Agreement
The Safe Harbour Agreement, established in the year 2000, allowed US companies to self-certify that they comply with the seven specified 'Safe Harbour' principles and thereby confirm that they will provide adequate protection for the personal data of EU citizens.

The Safe Harbour arrangement, as it stood, allowed firms to transfer data from the EU to the US if the US entities provided safeguards equivalent to those required by the EU's data-protection initiative. However, this agreement was accepted by the European Commission in 2000, a time when the internet was in its infancy and data flows much smaller.

The Safe Harbour Decision
The ECJ in its Decision stated that "legislation permitting [United States] public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life."

Essentially, the ECJ has declared that the Safe Harbour Agreement is no longer sufficient in the modern age of the internet, where huge volumes of personal data, often referred to as Big Data, are transferred between the continents on a daily basis. It has therefore invalidated the Agreement through the Safe Harbour Decision.

As a result of this ruling any organisation in the EU transferring data to a US organisation can no longer rely solely on the justification that the US organisation to which the European data is transferred is Safe Harbour certified. Likewise US organisations that are subject to the jurisdiction of the US Department of Commerce (DoC) can no longer rely on the automatic legitimacy that the Safe Harbour gave them to receive EU data.

Impact of the Safe Harbour Decision
Any company that is Safe Harbour certified is potentially affected by this decision. Indeed, there may be a wider, indirect impact on any organisation that has a US affiliated company or uses the services of a US company that is Safe Harbour certified. Over 4,000 companies are thought to be affected by the ruling.

In particular, this decision will have a huge effect on companies who deal with 'Big Data'. Big Data – the vast swathes of complex data that presents significant logistical challenges and is becoming more and more commonplace in today's digital society – is collected by multinationals around the globe. In order to make this data valuable, it needs to be stored and analysed

somewhere, typically centrally in order to derive meaningful analytics that respond to real business needs. Many large multinationals are headquartered in the US and collect data from a variety of sources around the globe in all the jurisdictions in which they operate, and transmit this data to data centres in the US where it is collated, processed and analysed in order to fulfil a multitude of functions: Google monitoring the search terms which will help it predict the next flu outbreak; Netflix recommending films based on their customer's viewing habits; or Target predicting future purchasing habits to advertise accordingly.

An example of the many uses of Big Data is Airbnb, the company revolutionising the travel industry through the "sharing economy". Airbnb links peoples' spare rooms and empty apartments with travellers around the globe. It allows hosts to set their own prices, but armed with billions of data points, the company is now starting to nudge hosts towards prices that earn them – and Airbnb – more money, advising on likelihoods of obtaining bookings at different prices and suggesting appropriate pricing based on huge amounts of data collected from previous bookings. Going forward this data could prove very valuable to Airbnb beyond their core offering – they are quietly building the most intelligent travel agent of all time. Vice President of Engineering, Mike Curtis stated that the company realised they had a lot of data that other people don't have. "We have travel patterns. We have the reviews. We have the descriptions of the listings. We know a lot about neighbourhoods". Using this data, they are beginning to offer travel recommendations based on who you are, and who knows how they will exploit the value inherent in the data they are collecting in the future. Of note: Airbnb, Inc. is certified as a Safe Harbour organisation. The San Francisco headquartered company operates across numerous European jurisdictions, collating data to be transferred to the US for storage, processing and analytics. This was formerly done under the auspices of the Safe Harbour Framework, but now Airbnb will have to find a workaround for its data transfers, unless and until a new framework is developed.

The future?

Steps are already being taken to address the issue, with the EU and US agreeing in principle on the development of a new data-transfer pact. Indeed, talks have been ongoing since January 2014 on the basis of a 2013 Commission paper on the functioning and shortcomings of the Safe Harbour Agreement. These talks have ramped up in the weeks following the Safe Harbour Decision to work out not only a new framework, but also an interim solution until such a framework is put in place. However, this will not be an easy task, given the vast changes in the digital landscape since the original framework was put in place. The legislators must find a solution that fits all the players. This includes not only the Silicon Valley giants and major multinational corporations, who have had the power to extract meaning and value from Big Data for some time, but also small and medium sized enterprises that now use and manipulate Big Data across continents in order to innovate and grow. All the while, the drafters must also ensure that the privacy protections enshrined in both the EU Charter of Fundamental Rights and the US Constitution are enshrined effectively.

Indeed, on 6 November 2015, exactly one month after the ruling, the European Commission made public a communication to the European Parliament and the Council reaffirming the importance of the "fundamental right to the protection of personal data". This communication also served as a further reminder of the difficulties the drafters of any new framework may come across, highlighting the need to protect privacy whilst respecting the fact that "transfers of personal data are an essential element of the transatlantic relationship".

Given these complications, a prospective deadline of three months has been set for the Commission and the US Government to conclude their discussions on the matter. There is, as of yet, no deadline set for the completion and implementation of a new framework.

In the interim the ruling is likely to have a significant impact and place significant responsibilities on those who process Big Data collated across the globe, with potentially complex new interim rules being established to fill the gap the Safe Harbour Decision has left.

If you or your organisation would like further information on the ruling or advice on how this may affect you, please do not hesitate to contact Guy Harvey, Nicola Rinaldi or Gordon Moir.

Follow us on Twitter @shepwedd for regular updates.