# End of Safe Harbour data protection rules isn't the end of the world – let's hope its successor is better

October 22 2015, by John Stevenson

The Safe Harbour agreement that reduced US firms compliance with European data protection rules to a tick-box exercise has been scrapped, leading to apocalyptic claims such as tech giants like Facebook closing their doors in Europe. While the ending of the long-established Safe Harbour framework is a blow for US firms looking for red tape-free opportunities in the EU, there are many other routes to doing business legally across the Atlantic.

## History of state surveillance

The self-regulatory Safe Harbour regime governing the transfer of personal data from the EU to the US has long been criticised for its ineffectiveness. One of the principles enshrined in the European Data Protection Directive is that personal data gathered for one purpose should not be used for another purpose. Numerous studies have highlighted the failure of companies to follow even the modest self-certifying requirements of Safe Harbor. Many participating companies do not publish up-to-date privacy policies, those that are published do not uphold all the data protection principles in the directive, while some companies fail to comply even with their own policies.

The approach to personal privacy across the Atlantic is very different. Legislation in the US is industry-based, with regulations specific to the health insurance industry for example. In Europe the approach has been

to apply data protection legislation across the board, in all industries across all member states. Because of the history of state surveillance of citizens in the post-war period there is considerable resistance in many European countries to the routine monitoring of electronic communications. Although national security is a compelling argument for the suspension of individual privacy rights, in its ruling the European Court of Justice decided that the mass surveillance conducted by the US National Security Agency as revealed by Edward Snowden's leaked files is not exempt in the way targeted surveillance might be.

## Cloud-based storage and processing services

There is an argument for self-regulation due to its lower burden on business and trade. But it also means EU consumers's personal data is transferred to a jurisdiction with fewer privacy protections. In a 2013 report the Federal Trade Commission indicated that there had been only 10 prosecutions for non-compliance in the US in the 13 years Safe Harbor had been in place. This included orders against Google, Facebook and Myspace to "prohibit these companies from misrepresenting their privacy practices and their participation in Safe Harbor or similar programs". In 2012 Google paid a fine of £22.5m to settle allegations that they had violated the terms of the order.

The ECJ's judgement could affect social media organisations such as Facebook and Google which have data processing centres both in and outside the EU. It could also affect companies operating across international boundaries, where staff information is centralised. However the largest category of affected organisations will be companies that make use of cloud-based storage and processing services – Google Docs or Microsoft Office 365, for example. Inevitably personal data will end up on the cloud and many of these depend on a distributed architecture to ensure resilience and ease of disaster recovery, which could be legally ambiguous. The UK regulator, the

Information Commissioner's Office, emphasises that the Safe Harbor framework is only one way of allowing transfer of personal data. Others include the use contracts such as End-User Licence Agreements (EULAs) used by software companies or other terms of service agreements. Binding corporate rules that ensure data protection principles are followed are also acceptable. Some international corporations have created European data centres which are ring-fenced to ensure that personal data is not transmitted outside the EU. Finally, there is always the option of individual consent, which might be a possibility for a smaller firm.

This judgement may influence the current debate on privacy and surveillance that is underway through forums such as the Electronic Frontier Foundation in the US and the Open Rights Group in the UK. How the striking down of Safe Harbour may influence the US-EU efforts to create a successor to it, not to mention the current Transatlantic Trade and Investment International Partnership (TTIP) negotiations, remains to be seen.

Provided by City University London