AmCham EU's position on the Safe Harbor Review

An analysis of the European Commission's review of the US-EU Safe Harbor Agreement

Executive summary

With over 4000 companies in both the EU and US certified under Safe Harbor it has become a vital mechanism for the transfer of personal data across the Atlantic. It is of utmost importance that policy-makers take the time to reflect and analyse concerns before implementing any changes that may cause any disruptions to this flow of data. Global companies rely on communication networks to deliver services to customers, run manufacturing and internal operations and manage global supply chains. AmCham EU members believe that the protection offered to data subjects via Safe Harbor is as robust as that afforded by national data protection enforcement regimes in the EU and suspension would severely impact both the EU and US economies.

* * *

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled €1.9 trillion in 2012 and directly supports more than 4.2 million jobs in Europe.

* * *

Brussels, 26 March 2014

American Chamber of Commerce to the European Union (AmCham EU)
Avenue des Arts 53, B-1000 Brussels, Belgium
Register ID: 5265780509-97
Tel: +32 (0)2 513 68 92 | www.amchameu.eu

Secretariat Point of Contact: Roger Coelho; rco@amchameu.eu; +32 (0)2 289 10 18

POSITION PAPER

Introduction

The Safe Harbor programme introduced in 2000 has become a widely-used system for businesses with more than 4000 certified organisations[1], including a large number of EU companies[2]. All these companies are certified for transferring personal data from Europe to Safe Harbor participants in the US. AmCham EU members have found Safe Harbor to be a useful tool that provides legal certainty and enables transatlantic business. The global economy cannot function without constant streams of data across borders, which has become a vital source of innovation and competitive advantage for all sectors. Global companies rely on communication networks to deliver services to customers, run manufacturing and internal operations and manage global supply chains.

AmCham EU members believe that the protection offered to data subjects via Safe Harbor is as robust as that afforded by national data protection enforcement regimes in the EU. Moreover, its success and popularity has led to a much greater awareness of EU data protection laws and necessary safeguards to be respected by companies transferring data to the US. It is therefore unfortunate that Safe Harbor has recently been subject to some ill-informed criticism. Companies that are certified are aware of their responsibilities and have internal or external compliance programmes. Issues of non-compliance with the Safe Harbor framework that have arisen are in fact mainly related to companies that falsely claim to have adhered to the Safe Harbor or failed to renew their certification.

Going forward, improvements could be made that would further increase the value of Safe Harbor. In this regard, AmCham EU members welcome the EU Commission's Communication of 27 November 2014[3] which includes a number of recommendations to better implement Safe Harbor.

We welcome the thrust of the recommendations made by the recent review which we feel will serve to further improve confidence in Safe Harbor. However, we are concerned in particular at the following recommendation that we consider will impose a significant regulatory burden on business without a consequent benefit to consumers:

> **Recommendation 3:** (asking the list of subcontractors) Safe Harbour certified companies should publish privacy conditions of any contracts they conclude with subcontractors, e.g. cloud computing services. In practice, this would entail that companies would have to publish and maintain an up-to-date list of all their subcontractors.

The current Safe Harbor framework already provides that certified companies can only transfer data to third parties such as subcontractors if the subcontractor (i) subscribes to the Safe Harbor principles, (ii) is subject to the Directive or another adequacy finding or (iii) enters into a written agreement providing 'at least the same level of privacy protection as is required by the relevant [Safe Harbor] Principles'. Recommendation 3 appears to ignore the existence of possibilities (i) and (ii) above, and seeks to impose a burdensome obligation on certified companies to publish the contractual conditions for each subcontractor, while this provides no clear benefit to the EU individuals concerned. In addition, providing the names as well as publishing the privacy conditions with such subcontractors would result in forcing Safe Harbor companies to disclose sensitive information in breach of their confidentiality obligations towards those suppliers. Indeed, generally the terms as well as the existence

[1] Of which 3246 are listed as 'current' (Commission Communication on the Functioning of the Safe Harbour, 27 November 2013).
[2] https://safeharbor.export.gov/list.aspx
[3] http://ec.europa.eu/justice/newsroom/data-protection/news/131127_en.htm

of such contracts are confidential between the parties. Finally, such requirement would go beyond what is required from companies under EU data protection law.

Regarding the questions raised by the US intelligence agencies' access to data, managing the scope of government surveillance and using data for commercial purposes are two different issues. Unfortunately, over the last months many have mixed both up. Concerns regarding the NSA Surveillance revelations should remain a government-to-government discussion regarding government access to data. Safe Harbor is designed for commercial data flows and is essential for businesses and consumers on both sides of the Atlantic.

Moreover, recommendations 12 and 13 would exceed the areas of EU competence, since national security issues remain the sole responsibility of the Member States. Also, they would cause serious implementation issues and impose conflicting requirements upon Safe Harbor companies:

> **Recommendation 12**: Privacy policies of self-certified companies should include information on the extent to which US law allows public authorities to collect and process data transferred under the Safe Harbour. In particular companies should be encouraged to indicate in their privacy policies when they apply exceptions to the Principles to meet national security, public interest or law enforcement requirements.

While many Safe Harbor Policies transparently disclose that they may be subject to a national security, public interest, or law enforcement exception (in line with the Safe Harbor Principles), disclosing details about when they apply such exceptions is generally not allowed under US law, as it is equally not allowed under EU law to disclose which data companies are compelled to share with public authorities. Also, it is not for private companies to provide an overview of the extent to which US law allows public authorities to subpoena data.

> **Recommendation 13**: It is important that the national security exception foreseen by the Safe Harbour Decision is used only to an extent that is strictly necessary or proportionate.

While Safe Harbor companies should of course ensure they only disclose data which they are legally compelled to disclose under enforceable subpoenas, it is not for private companies to challenge the necessity and proportionality of law enforcement policies as pursued by public authorities.

In addition to the recommendations, one aspect that could be explicitly confirmed is that data processors established in the US can also apply for Safe Harbor certification. Data processors' certifications apply the principle of data security, which is something they can control themselves. To comply with the other Safe Harbor principles they require the cooperation of the European data controllers (their clients). Such a certification by a data processor offers an adequate legal basis to Safe Harbor companies which receive personal data from their clients located in the EU and need to process it.

To conclude, AmCham EU does not support the calls for a suspension of Safe Harbor. While Safe Harbor rules continue to offer solid protections and do not need a major makeover, after 13 years, a review that seeks to achieve meaningful improvements in its implementation would be welcome.