Scrapping Safe Harbor: European scare mongering or a real possibility?

Bridget Treacy, Partner, and Anita Bapat, Associate with Hunton & Williams, review the criticisms of Safe Harbor and assess its future as an 'adequate' data transfer mechanism

Since last year's PRISM revelations and US law enforcement agencies' access to EU personal data, Safe Harbor, the self certification scheme which permits transfers of personal data from the EU to the US has come under close scrutiny. Are calls for it to be scrapped simply EU scare mongering, or a real likelihood? In this article, we examine what the Safe Harbor framework is, review its criticisms and the steps being taken to address them, and assess the future of Safe Harbor as an adequate data transfer mechanism under European data protection law.

What is Safe Harbor?

Directive 95/46/EC (the 'Data Protection Directive') prohibits organisations from transferring personal data from the EU to countries outside the European Economic Area ('EEA'), unless there is an adequate level of data protection (subject to limited exceptions).

Readers will recall that the Safe Harbor framework is one transfer mechanism permitted under the Data Protection Directive that allows companies that have certified to it to transfer data freely from the EU to the US. In order to certify, an organisation must ensure that its personal data practices adhere to the Seven Safe Harbor Privacy Principles, namely:

- **Notice** – individuals must be given notice of the purpose and collection of personal data;
- **Choice** — individuals must be given the opportunity to choose (i.e., opt-out) whether their personal data will be disclosed to a third party or used for a different purpose. For sensitive data, opt-in is required;
- **Onward Transfer** – Safe Harbor certified organisations must ensure that third parties that receive personal data are bound to follow the Safe Harbor Privacy Principles, or their equivalent;
- **Access** — individuals must have access to their information to correct, amend or delete it;
- **Security** — organisations must take reasonable precautions to protect personal information from loss, misuse and unauthorised access, disclosure, alteration and destruction;
- **Data integrity** — organisations must take reasonable steps to ensure the data are reliable for their intended use, and are accurate, complete and current; and
- **Enforcement** — organisations must make available recourse mechanisms to investigate and resolve the complaints of individuals, remedy problems arising from any failure to comply, and conduct annual objective verifications of their compliance with the Safe Harbor Privacy Principles.

Organisations must file a self-certification form with the Department of Commerce ('DoC') and publish a Safe Harbor privacy policy that states how it complies with Safe Harbor.

In order to maintain their Safe Harbor certifications, organisations must annually verify and recertify their compliance with the Safe Harbor Privacy Principles.

How does the US enforce Safe Harbor?

Onward transfers under Safe Harbor are subject to US law and to the oversight of the Federal Trade Commission ('FTC') or (for US carriers and ticket agents) the Department of Transportation ('DoT'). However, an EU Data Protection Authority ('DPA') can raise questions or concerns about the compliance of a transfer made pursuant to Safe Harbor.

The FTC has brought a number of enforcement actions asserting violations of the Safe Harbor commitments, including high-profile actions against MySpace LLC, Facebook, Inc. and Google, Inc. In 2014, there have been several instances of enforcement action by the FTC, including:

- in January 2014, the FTC announced settlements with 12 companies that allegedly falsely claimed they complied with Safe Harbor, even though there were no substantive violations of the Safe Harbor Privacy Principles;
- in February 2014, the FTC announced a proposed settlement with Fantage.com for allegedly

deceptively claiming in its privacy policy that it held a current Safe Harbor certification, when in fact its certification had lapsed in June 2012;

- in May 2014, the FTC announced a settlement with clothing manufacturer American Apparel related to charges that the company falsely claimed to comply with Safe Harbor, even though it had allowed the certification to expire; and
- in November 2014, the FTC announced that data privacy certifier True Ultimate Standards Everywhere, Inc. ('TRUSTe') agreed to settle charges that the company deceived consumers about its Safe Harbor recertification program.

Despite these enforcement actions, many in the EU have expressed concern about whether Safe Harbor's self-certification procedure is adequate.

What criticisms have been made in the EU of Safe Harbor?

Since 2010, some EU DPAs have expressed concern about third-party access to personal data transferred from the EU to the US under Safe Harbor.

In 2010, the Dusseldorf Kreis, a working group comprised of 16 German state DPAs that are responsible for the private sector, issued a resolution requiring German data exporters to exercise additional diligence when transferring data to Safe Harbor-certified organisations, and prohibited German data exporters from relying solely on Safe Harbor in order to transfer data to the US.

By requiring additional diligence, the resolution appeared to question Safe Harbor, and whether the system was sufficient to demonstrate an adequate level of protection for personal data. Similarly, an Article 29 Working Party Opinion on cloud computing published in 2012 concluded that EU data exporters cannot rely solely on Safe Harbor certification.

EU criticism intensified in June 2013 following the disclosure of the US government's surveillance program, PRISM, which allegedly gave the US National Security Agency access to personal data that was transferred to online service providers in the US under Safe Harbor.

> ***"It appears that while there is general agreement on most of the recommendations, the parties are finding it challenging to reach agreement on the issue of US authorities' access to EU personal data."***

Further EU criticism of Safe Harbor was voiced during the Transatlantic Trade and Investment Partnership ('TTIP') negotiations (which aim to establish a free trade agreement between the US and the EU). In July 2013, the Conference of the German Data Protection Commissioners, including both federal and state Commissioners, issued a press release stating that surveillance activities by foreign intelligence and security agencies threaten international data traffic between Germany and countries outside the EEA.

In light of these recent developments, the German Commissioners decided to stop issuing approvals for international data transfers until the German government can demonstrate that unlimited access to German citizens' personal data by foreign national intelligence services complies with fundamental principles of data protection law (namely, necessity, proportionality and purpose limitation).

In contrast with the German Commissioners, following the PRISM disclosures, the Irish Office of the Data Protection Commissioner ('ODPC') did not call Safe Harbor into question or impose additional compliance requirements on Irish data exporters transferring data to Safe Harbor-certified importers. In its response to formal complaints at the time, the ODPC stressed 'that an Irish-based data controller has met their data protection obligations in relation to the transfer of personal data to the US if the US based entity is 'Safe Harbor' registered.' The ODPC also emphasised that under Safe Harbor, onward transfers are permitted for purposes of law enforcement. The approach of the ODPC reinforced the validity of Safe Harbor as a valid data transfer mechanism, and sent a message that it is here to stay.

In light of concerns following the PRISM revelations, the European Parliament called on the European Commission (the 'Commission') to review Safe Harbor and asked the Commission to consider whether to suspend or reverse Safe Harbor as an adequate data transfer mechanism. These calls from the European Parliament and German Commissioners led to the heightened rhetoric surrounding Safe Harbor and to speculation that it might be suspended. The Commission completed its review in November 2013, and made a number of recommendations, which are described below.

Can Safe Harbor be reversed or suspended?

Following the recent criticism, there has been much speculation surrounding calls for the Commission to reverse or suspend Safe Harbor. However, it is not clear whether the Commission is empowered to do so under current circumstances, given that no DPA has suspended Safe Harbor data flows.

Under Article 3(4) of Decision 2000/520/EC, if a national DPA suspends a Safe Harbor data flow and provides evidence that the FTC is failing to ensure compliance with the Safe Harbor Principles, the Commission must inform the DoC and may present draft measures aimed at reversing, suspending

(Continued on page 6)

(Continued from page 5)

or limiting the scope of Decision 2000/520/EC. Article 3(3) of Decision 2000/520/EC requires both the Commission and individual DPAs to inform each other of any instances where the FTC is failing to ensure compliance with the Safe Harbor Privacy Principles.

Article 3(4) appears to authorise the Commission to take action only where a national DPA has first suspended Safe Harbor data flows. To date, no DPA has done so, although the recent decision of the German federal and state DPAs comes close (see above).

What improvements have been suggested to Safe Harbor?

The Commission's analysis of Safe Harbor concluded that the current framework lacks transparency and active enforcement, resulting in some Safe Harbor self-certified companies not complying with the Safe Harbor Privacy Principles in practice. The Commission believes that Safe Harbor should be revised, and made 13 recommendations aimed at improving the transparency of Safe Harbor and increasing active enforcement through audits and monitoring.

The Commission's recommendations address four key areas:

Transparency:

- self-certified companies should publicly disclose their privacy policies;
- online Safe Harbor privacy policies should include a link to the DoC's Safe Harbour list of current Safe Harbor members;
- self-certified companies should publish privacy conditions of any contracts they conclude with subcontractors; and
- the DoC's Safe Harbor list should clearly flag those companies that are not current members.

Redress:

- online Safe Harbor privacy policies should include a link to the chosen Alternative Dispute Resolution ('ADR') provider;
- the ADR choice should be readily available and affordable; and
- the DoC should systematically monitor ADR providers, specifically in relation to the transparency and accessibility of their procedures and how they follow up complaints.

Enforcement

- Safe Harbor members should be subject to spot check 'ex officio' investigations, in order to verify the substantive compliance of their privacy policies;
- follow-up investigations after one year, where there has been a finding of non-compliance, should be implemented;
- the DoC should inform the competent EU DPA of pending complaints and suspected non-compliance; and
- allegations of false claims of Safe Harbor adherence should be investigated.

Access by US authorities:

- Safe Harbor privacy policies should specify the extent to which US law allows public authorities to collect and process data transferred under Safe Harbor; and
- the national security exception under Safe Harbor should be used only to the extent strictly necessary or proportionate.

Will any changes be made to Safe Harbor?

The DoC has repeatedly asserted the importance of Safe Harbor and in January 2014, the DoC's International Trade Administration published a Key Points document highlighting the benefits, oversight and enforcement of the US-EU and US-Swiss Safe Harbor regimes.

In addition to this, the DoC and the Commission have been working together to implement the 13 recommendations set out above and have made significant, if slow, progress. The recommendations were expected to be implemented during the Summer of 2014, but this is still in progress. It appears that while there is general agreement on most of the recommendations, the parties are finding it challenging to reach agreement on the issue of US authorities' access to EU personal data. Further, the change in administration in the EU institutions following the European elections in May 2015 has also slowed progress.

Whilst US officials have insisted that they hope to be able to pick up where they left off under the previous Commission, no specific timeline has been set. That said, the new President of the European Commission has asked his new Vice-President for the Digital Single Market, Andrus Ansip, to complete the review of Safe Harbor by April 2015.

Conclusion

Despite the negative publicity, it seems unlikely that Safe Harbor will be suspended, and even less likely that the Commission's Decision 2000/520/EC on Safe Harbor will be reversed.

Almost 5,000 organisations are certified to Safe Harbor. Suspending or reversing it would cause considerable uncertainty for businesses, and would disrupt numerous existing business arrangements between the EU and US. In addition, the key issue which has arisen in the Safe Harbor debate (and which is apparently still under negotiation), is that of law enforcement access to personal data. This issue is not confined to Safe Harbor, but arises in the context of other data transfer mechanisms, such as adequacy decisions, Model Clauses and Binding Corporate Rules.

We await the Commission's and DoC's plans for Safe Harbor in 2015.

Bridget Treacy and Anita Bapat
Hunton & Williams
btreacy@hunton.com
abapat@hunton.com