Privacy & Data Security: The Future of the US-EU Safe Harbor

NAOMI MCBRIDE, LISA J. SOTTO AND BRIDGET TREACY, HUNTON & WILLIAMS LLP, WITH PRACTICAL LAW US INTELLECTUAL PROPERTY & TECHNOLOGY AND UK IP&IT

An article examining the safe harbor for transferring personal data from the EU to the US and its future viability in light of criticism from the European Commission and some EU data protection authorities, which has intensified following disclosure of the US government's surveillance programs.

The US-EU Safe Harbor framework is an important cross-border data transfer mechanism that enables certified organizations to transfer personal data from the EU to the US in compliance with European data protection laws. Almost 3,500 organizations across a broad range of industries are Safe Harbor-certified.

Recently, however, the Safe Harbor's future has been thrown into doubt. Following widespread concern about the US government's covert surveillance programs, European Commission Vice-President Viviane Reding announced in July 2013 a European Commission (Commission) plan to review the Safe Harbor and publish the results before the end of 2013. She observed that the Safe Harbor "may not be so safe after all," noting that it "could be a loophole" for data transfers because "it allows data transfers from EU to US companies – although US data protection standards are lower than our European ones."

While it seems unlikely that the Safe Harbor will be suspended or reversed, companies in both the US and EU should closely monitor the political landscape. This article examines:

- The Safe Harbor framework, including the Commission's adequacy requirement and how onward transfers are made under the Safe Harbor.
- US enforcement of the Safe Harbor.
- EU concerns about the Safe Harbor and actions taken in response to these concerns.
- Key points in the debate on the Safe Harbor's viability.

THE US-EU SAFE HARBOR FRAMEWORK

The EU Data Protection Directive (Directive 95/46/EC), with limited exceptions, generally prohibits organizations from transferring personal data from the EU to countries outside the European Economic Area (EEA) unless there is an adequate level of data protection. Under Directive 95/46/EC, the adequacy requirement is met if the Commission recognizes that the data recipient's country's laws provide an adequate level of data protection. If the Commission does not recognize the country as providing adequate protection:

- The data recipient can include in its contract with the data exporter standard contractual clauses published by the Commission and approved or adopted under national law.
- The data recipient can comply with the Safe Harbor, a set of privacy principles (Safe Harbor Principles) and Frequently Asked Questions (FAQs) that the US Department of Commerce developed in collaboration with the Commission to meet the adequacy requirement. The Safe Harbor Principles address notice, choice, onward transfer, security, data integrity, access and enforcement.
- If the data transfer takes place between different entities from the same group of companies, the group may adopt binding corporate rules (BCRs) that allow it to meet the requirements of Directive 95/46/EC.

For more information on transfer mechanisms, see *Article, Solutions to the cross-border transfers of personal data from the EEA (http://us.practicallaw.com/3-385-6772)*.

As a country, the US does not meet the EU adequacy requirement. However, the Safe Harbor provides a mechanism for a US data importer that complies with the Safe Harbor framework to receive personal data from organizations located in the EEA. The Safe Harbor's onward transfer principle sets out the requirements for a service provider (or other third party) to receive personal data that originated in the EU from a US entity that has certified to the Safe Harbor (see *Onward Transfers under the Safe Harbor*).

For more information on Directive 95/46/EC, see *Practice Note, Overview of EU data protection regime (http://us.practicallaw.com/8-505-1453)*. For more information on US privacy and data security law, see *Practice Note, US Privacy and Data Security Law: Overview (http://us.practicallaw.com/6-501-4555)*.

To certify to the Safe Harbor, an organization must:

- Conform its relevant personal data practices to the Safe Harbor framework.
- File a self-certification form with the Department of Commerce.
- Publish a Safe Harbor privacy policy that states how the organization complies with the Safe Harbor.

An organization must also annually verify and recertify its compliance with the Safe Harbor Principles.

The US Department of Commerce's International Trade Administration (ITA) provides information on the Safe Harbor, including requirements for certification, on its *website*. For a model Safe Harbor privacy policy, see *Standard Document, Safe harbor policy (http://us.practicallaw.com/6-524-1888)*.

ONWARD TRANSFERS UNDER THE SAFE HARBOR

After EU personal data are transferred to a Safe Harbor-certified US entity, further transfers from the importer to a third party (onward transfers) are subject to restrictions under the Safe Harbor. With limited exceptions, under the Safe Harbor a certified entity generally may disclose the personal data to a third party only under the following circumstances:

- The third party is acting as the certified entity's agent (that is, performing tasks on behalf of and under the instructions of the entity) and:
  - subscribes to the Safe Harbor Principles;
  - is itself subject to Directive 95/46/EC; or
  - enters into a written agreement requiring it to provide at least the level of protection required by the Safe Harbor Principles.
- If the third party is not the certified entity's agent, the data must be disclosed in accordance with the Safe Harbor's notice and choice principles. This means the certified entity may transfer personal data only if the affected data subjects have been:
  - notified about the types of third parties to whom the data may be disclosed; and
  - given the opportunity to opt out of those disclosures.

Disclosing personal data in accordance with the Safe Harbor's notice and choice principles can be difficult to implement in cases where the Safe Harbor-certified entity does not have a direct contractual relationship with the affected data subjects.

US ENFORCEMENT OF THE SAFE HARBOR

Onward transfers under the Safe Harbor are subject to US law and Federal Trade Commission (FTC) oversight. However, an EU data protection authority (DPA) also can raise questions about compliance of an onward transfer made pursuant to the Safe Harbor, including:

- Questions of procedural compliance (for example, evidence of Safe Harbor certification).
- Questions of substantive compliance with the obligations imposed on the data exporter under local law (for example, entering into data processing agreements with processors).

The Safe Harbor's enforcement framework arguably is sufficient to correct any non-compliance without resort to enforcement action by EU DPAs. The Safe Harbor's enforcement principle sets out an escalation procedure that encourages individuals first to address their complaints directly with the Safe Harbor-certified organization itself. These complaints typically are directed to the organization's chief privacy officer. If the organization does not sufficiently address the complaint, individuals may then seek to have them addressed by a third-party dispute resolution body, such as the American Arbitration Association. The dispute resolution body:

- Is selected by the Safe Harbor-certified organization.
- May order a range of remedies and sanctions for an organization's failure to comply with the Safe Harbor, including:
  - publicity for findings of non-compliance;
  - requiring the organization to delete data in certain circumstances;
  - suspending certification and removing a privacy seal;
  - monetary compensation to individuals for losses incurred as a result of the non-compliance; and
  - injunctive orders.

Some privacy advocates have expressed concerns that this process can be prohibitively expensive for individuals.

If the organization fails to comply with the dispute resolution body's ruling, the FTC may take action. The FTC is responsible for determining whether any alleged non-compliance constitutes an unfair or deceptive act or practice under Section 5 of the *Federal Trade Commission Act (http://us.practicallaw.com/6-383-6476)* (FTC Act). If the FTC concludes that it has reason to believe Section 5 has been violated, it may seek an administrative cease and desist order prohibiting the challenged practice or file a complaint in a federal district court seeking a federal court order to the same effect. If an administrative order is violated, the FTC may seek civil monetary penalties. For information about FTC regulation of privacy and data security under the FTC Act, see *Practice Note, US Privacy and Data Security Law: Overview: Federal Trade Commission Act (FTC Act) (http://us.practicallaw.com/6-501-4555#a591738)*.

The FTC has brought a number of enforcement actions asserting violations of Safe Harbor commitments, including high-profile actions against MySpace LLC, Facebook, Inc. and Google, Inc. Despite this, many in the EU have expressed concern about whether the Safe Harbor's self-certification procedure is adequate. One 2013 study indicated that 427 organizations claimed on their websites to be members of the Safe Harbor when they were not current members. Although the study intended to use this finding to discredit the Safe Harbor, the false assertions of these organizations did not, in fact, constitute a violation of the Safe Harbor (though they may constitute a deceptive trade practice in violation of Section 5 of the FTC Act). The 2013 study also indicated that more than 30% of Safe-Harbor-certified organizations did not identify an independent dispute resolution process for individuals. This too does not constitute a substantive violation of the Safe Harbor, though it does serve to fuel the rhetoric regarding concerns about the framework's adequacy.

EU ATTACKS ON THE SAFE HARBOR

For some time, EU DPAs and EU data exporters have expressed concern about third-party access to personal data transferred from the EU to the US under the Safe Harbor. EU criticism has intensified following disclosure of PRISM, the US government's surveillance program, which reportedly gave the National Security Agency access to personal data that was transferred to online service providers in the US under the Safe Harbor.

2010 DÜSSELDORFER KREIS RESOLUTION

The Düsseldorfer Kreis, a working group comprised of 16 German state DPAs that are responsible for the private sector, issued a resolution on April 29, 2010, requiring German data exporters to exercise additional diligence when transferring data to Safe Harbor-certified organizations. By requiring additional diligence, the resolution appeared to question the Commission's decision that Safe Harbor certification is sufficient to demonstrate an adequate level of protection for personal data.

Specifically, the resolution prohibits German data exporters from relying exclusively on Safe Harbor certification to determine whether a US data importer provides an adequate level of protection. German data exporters must also verify whether the data importer complies with certain minimum Safe Harbor requirements by:

- Verifying that the organization's certification is still valid.
- Ensuring that the organization complies with the Safe Harbor's notice principle, by providing notice of the data processing to relevant individuals.
- Documenting its assessment of the organization's adequacy under the Safe Harbor in order to be able to provide proof, if requested, by a German DPA.

The resolution recommends that a German data exporter:

- Use standard contractual clauses or BCRs to ensure adequate protection if it doubts the importer's Safe Harbor compliance following an assessment.
- Inform the appropriate DPA if:
  - it determines that an organization's Safe Harbor certification is no longer valid;
  - the organization does not provide required processing notice to individuals; or
  - it discovers other violations of the Safe Harbor Principles during the assessment.

A German data exporter may face sanctions if it fails to carry out the required assessment and transfers data to a US Safe Harbor-certified organization that does not meet the required standards.

Consequently, the Safe Harbor does not present a simple solution for German data exporters in the private sector as they are required to conduct further due diligence checks prior to commencing any data transfers.

2012 ARTICLE 29 WORKING PARTY OPINION ON CLOUD COMPUTING

The Article 29 Working Party adopted an opinion on cloud computing on July 1, 2012. It concluded that EU data exporters cannot rely solely on Safe Harbor certification.

According to the Working Party, to rely on Safe Harbor transfers to cloud vendors located in the US, a data exporter must obtain evidence of the US organization's:

- Self-certification.
- Compliance with the Safe Harbor, in particular with the notice principle.

The July 2012 opinion states that "sole self-certification with Safe Harbor may not be deemed sufficient in the absence of robust enforcement of data protection principles in the cloud environment." It also emphasizes that the data exporter must enter into a data processing agreement with the cloud vendors regardless of the data transfer mechanism.

RESPONSES TO PRISM AND OTHER LAW ENFORCEMENT ACCESS TO PERSONAL DATA

In June 2013, there were reports of US and EU authorities intercepting and accessing the electronic communications of EU citizens on an extensive scale, in part, pursuant to the PRISM program. Following these reports, in July 2013 the European Parliament called on the Commission to review the Safe Harbor. The European Parliament:

- Claimed that the PRISM program and US law enforcement agencies' access to personal data originating from the EU are serious violations of the Safe Harbor Agreement.
- Invited the Commission to reverse or suspend the Safe Harbor adequacy decision.

Further to her comments concerning the Commission plan to review the Safe Harbor, Vice-President Reding announced that the Commission would present a "solid assessment" of the Safe Harbor framework to ministers before the end of 2013. She referred to the revelations regarding the PRISM program as a "wake-up call" to which the EU's ongoing data protection reforms are "Europe's answer."

2013 Decision of the German DPAs

On July 24, 2013, the Conference of the German Data Protection Commissioners at both the federal and state levels 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 recent developments, the German Commissioners decided to:

- Stop issuing approvals for international data transfers until the German government demonstrates that unlimited access to German citizens' personal data by foreign national intelligence services complies with fundamental principles of data protection law (that is, necessity, proportionality and purpose limitation).
- Review whether to suspend data transfers carried out pursuant to the Safe Harbor.

The press release stated that the Commission has always stressed that national supervisory authorities may suspend data transfers if there is a "high probability" that the Safe Harbor Principles are being violated. The German Commissioners:

- Asserted that national security and law enforcement exceptions to compliance with the Safe Harbor Principles should be applied narrowly and used only as necessary.

- Suggested that the Commission issue an indefinite suspension of its decision concerning the Safe Harbor.

2013 Decision of the Irish DPA

In contrast with the German Commissioners, following the PRISM disclosures, the Irish Office of the Data Protection Commissioner (ODPC) did not call the Safe Harbor into question or impose additional compliance requirements on Irish data exporters transferring data to Safe Harbor-certified importers. In a letter of response to formal complaints, 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 the Safe Harbor, onward transfers are permitted for purposes of law enforcement.

Commission's Proposed Data Protection Regulation

On January 25, 2012, the Commission released proposed revisions to the EU data protection framework comprised of a General Data Protection Regulation (Regulation) and a Police and Criminal Justice Directive. Together they would repeal and replace Directive 95/46/EC. The Regulation is currently being negotiated. The Regulation's final form and when it may be adopted are unclear. In particular, the European Parliament (Parliament) recently passed a vote on a compromise text that departs significantly from the Commission's original draft.

If adopted, the Regulation would take direct effect in all 28 EU Member States and would significantly alter the current EU data protection framework. As initially proposed, notable changes include that:

- The Commission would be able to make adequacy findings about territories or processing sectors in a country outside the EU.
- Individual DPAs would be able to approve standard contractual clauses, in addition to the Commission-approved standard contractual clauses.
- BCRs would be formally recognized.

Under Article 41(8) of the Regulation, adequacy decisions made under Articles 25(6) or 26(4) of Directive 95/46/EC, including the Safe Harbor, would remain in force unless amended, replaced or repealed by the Commission.

Under the Parliament's compromise text, the Safe Harbor and other adequacy findings of the Commission would only remain in force for a period of five years after the adoption of the Regulation, unless amended, replaced or repealed by the Commission. The Parliament's compromise text also proposes an additional transfer basis in the form of "European Data Protection Seals", which would enable certified organizations to rely on privacy seals as an adequate basis for transfers outside of the EEA. Significantly, likely as a direct result of the PRISM revelations, the compromise text prohibits the disclosure of personal data as ordered by a court, tribunal or administrative authority of a country that is not deemed "adequate" by the Commission. Under this provision, if the US government were to request that a business (for example, a search engine, social network or cloud provider) disclose personal data processed in the EU, the business would be required to:

- Notify the DPA of the request without undue delay.
- Obtain the DPA's prior authorization for the transfer.

In virtually every instance, this provision would prohibit organizations from complying with governmental orders (often subject to criminal penalties) to disclose personal data.

Leaked unofficicial versions of the Council of the European Union's compromise proposals indicate that the Safe Harbor and other adequacy findings of the Commission would remain in force unless amended, replaced or repealed by the Commission, and similarly include additional adequacy bases for transfers on grounds of approved codes of conduct and certification mechanisms.

REVERSAL OR SUSPENSION OF THE SAFE HARBOR UNLIKELY

Following the PRISM disclosures, there has been considerable debate about the future of the Safe Harbor, and speculation that EU DPAs may no longer recognize it as a valid data transfer mechanism. Many have speculated that the Safe Harbor may be reversed or suspended, but those options are unlikely in practice.

SUSPENSION OF SAFE HARBOR DATA TRANSFERS BY NATIONAL DPAS

National DPAs have only limited authority to suspend data transfers based on the Safe Harbor. Article 3(1) of the Commission's Decision 2000/520/EC identifies only the following limited circumstances in which EU DPAs may suspend a data transfer to a Safe Harbor-certified recipient:

- There is a pending FTC enforcement action against the Safe Harbor-certified organization.
- A substantial likelihood exists that the Safe Harbor Principles are being violated and:
  - there is a reasonable basis for believing that the Safe Harbor enforcement mechanisms are not taking or will not take adequate timely steps;
  - permitting the transfer to proceed would create imminent risk of grave harm; and
  - the DPA has made reasonable efforts to liaise with the Safe Harbor-certified organization.

Decision 2000/520/EC describes these circumstances as exceptional and states that any suspension of data flows must be "justified, notwithstanding the finding of adequate protection." Except where there is FTC enforcement action, the test described above sets a high bar.

A national DPA's decision to suspend data transfers would be a serious step and one likely to cause significant controversy. To date, no DPA has done so, although the recent decision of the German federal and state DPAs comes close (see above, 2013 Decision of the German DPAs).

REVERSAL OR SUSPENSION OF SAFE HARBOR ADEQUACY DECISION

While the European Parliament's July 2, 2013 motion invites the Commission to reverse or suspend the Safe Harbor, it is not clear that the Commission is empowered to do so under current circumstances where no DPA has suspended Safe Harbor data flows under Articles 3(1)-(3) of Decision 2000/520/EC.

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 European Commission:

- Must inform the Department of Commerce.
- May present draft measures aimed at reversing, suspending 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 Principles.

Article 3(4) appears to authorize the Commission to take action only where a national DPA has first suspended Safe Harbor data flows.

DEPARTMENT OF COMMERCE RESPONSE

The Department of Commerce has repeatedly asserted the importance of the Safe Harbor.

Notwithstanding the resolution of the Düsseldorfer Kreis and the opinion of the Working Party, in April 2013 the Department of Commerce's International Trade Administration (ITA) issued a guidance document where it confirmed the Safe Harbor as a legitimate transfer mechanism for cloud vendors on the basis that cloud computing does not represent any unique issues for Safe Harbor. The ITA concluded that "[t]he existing Safe Harbor Privacy Principles are comprehensive and flexible enough to address the issues raised by the cloud computing model...."

Former US Secretary of Commerce Cameron Kerry has emphasized the value of the Safe Harbor framework for both the EU and the US. In a 2012 editorial, Mr. Kerry wrote that "[t]he value of this mechanism cannot be overstated." He explained that, "[t]he US and EU privacy regimes differ because their legal systems and political structures are distinct, but our values are similar." He continued that "[t]he US and the EU ultimately share the same goals - to protect privacy and facilitate trade and economic growth." In a Department of Commerce data privacy seminar in March 2013, Mr. Kerry once again noted the importance of the Safe Harbor in strengthening the relationship between the US and the EU.

Mr. Kerry maintained his support for the Safe Harbor in the face of EU criticism after the PRISM disclosures. In his final speech as Secretary of Commerce in August 2013, Mr. Kerry warned that preventing the sharing of data between the EU and the US "would cause significant and immediate economic damage."

FINAL THOUGHTS

Despite the rhetoric, it seems unlikely that the Safe Harbor will be suspended, and even less likely that the Commission's Decision 2000/520/EC on the Safe Harbor will be reversed. Any such action would cause considerable uncertainty and would disrupt existing business arrangements that fuel the global economy. In addition, talk of suspending or reversing the Safe Harbor to address law enforcement access to personal data is misplaced. These issues are not specific to the Safe Harbor. They also arise in the context of other data transfer mechanisms, such as adequacy decisions, model clauses and BCRs.

12-13