Key Points Concerning the Benefits, Oversight, and Enforcement of Safe Harbor

These key points, which have been prepared by the U.S. Department of Commerce's International Trade Administration (ITA), provide useful information about the benefits, oversight, and enforcement of the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks (hereinafter "Safe Harbor").

Safe Harbor provides significant economic benefits not only to the U.S. economy, but also to the EU and Swiss economies.

A report recently published by European Centre for International Political Economy (ECIPE) found that, "If services trade and cross-border data flows are seriously disrupted (assuming that binding corporate rules, model contract clauses and EU-U.S. Safe Harbor framework are no longer recognized), the negative impact on EU GDP could reach -0.8% to -1.3%. EU services exports to the United States drop by -6.7% due to loss of competitiveness."[1]

Many U.S. organizations that self-certify to Safe Harbor do so at the express request of European customers/clients or partners, while others are actually U.S. subsidiaries or divisions of European organizations. For example, U.S. subsidiaries of Alcatel-Lucent (France), AstraZeneca Pharmaceuticals (UK), BAE Systems (UK), Bayer (Germany), Bertelsmann (Germany), Dassault Systèmes (France), Ericsson (Sweden), Nokia (Finland), and Novartis (Switzerland) are all participants in Safe Harbor.

Approximately half of the organizations that have self-certified under Safe Harbor have indicated that they receive "organization human resources data" (i.e., personal information about their employees, past or present, collected in the context of the employment relationship); therefore, Safe Harbor enables U.S. organizations to process data required to employ EU/EEA and/or Swiss citizens.

Safe Harbor's economic benefits are realized across a vast array of manufacturing and service sectors in the U.S., EU, and Swiss economies. Safe Harbor participants, 60% of which are small or medium-sized enterprises, have self-identified their participation in 102 different industry sectors. More than 4,000 organizations have self-certified to Safe Harbor since its inception, over 3,000 of which remain active participants; nevertheless, the number of organizations that benefit from Safe Harbor and are required to adhere to its privacy principles is far greater. Many Safe Harbor organizations serve as multipliers with contracts binding other organizations to provide at least the same level of privacy protection as required by the relevant Safe Harbor Privacy Principles.

Claims of Safe Harbor participation can easily be verified by searching the official Safe Harbor List(s) to determine whether a given organization is on the List(s), and if it is, whether its "Certification Status" is "Current" or has lapsed. The public Safe Harbor List(s) clearly indicate which organizations are assured of the benefits of Safe Harbor (i.e., the presumption of "adequacy").

---

[1] *See*, "The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce" European Centre for International Political Economy (ECIPE), March 2013. Available at: http://www.uschamber.com/reports/economic-importance-getting-data-protection-right

The ITA maintains a list, which is updated regularly, of those organizations that have self-certified their compliance with the U.S.-EU Safe Harbor Framework, as well as a list of those organizations that have self-certified their compliance with the similar, but separate U.S.-Swiss Safe Harbor Framework. The Safe Harbor Lists are publicly available on the U.S. Department of Commerce Safe Harbor website (i.e., export.gov/safeharbor).

Compliance with the U.S.-EU Safe Harbor Framework and the U.S.-Swiss Safe Harbor Framework requires that each organization that has self-certified its adherence to the relevant Framework(s) (i.e., the Safe Harbor Privacy Principles and the Frequently Asked Questions and answers that clarify and supplement the Principles) reaffirm its commitment each year no later than the anniversary of the date on which its original self-certification was finalized.

If an organization does not complete the re-certification process in a timely manner in accordance with the requirements specified in the Framework(s) and guidance provided by the ITA, its "Certification Status" will lapse (i.e., it will change from "Current" to "Not Current"). An organization's "Certification Status" will remain "Not Current" until it has satisfactorily addressed the underlying reasons for the lapse and has complied with the requirements for re-certification. An organization will not be assured of the benefits of the Safe Harbor (i.e., the presumption of "adequacy") for so long as it remains "Not Current"

When Safe Harbor was negotiated it was agreed that it was important to maintain "Not Current" organizations on the public list(s), as those organizations remain responsible for protecting data collected during their participation in Safe Harbor. The undertaking to adhere to the Safe Harbor Privacy Principles is not time-limited in respect of data received during the period in which an organization enjoys the benefits of the Safe Harbor. An organization's undertaking means that it will continue to apply the Principles to such data for as long as the organization stores, uses or discloses them, even if it subsequently leaves the Safe Harbor for any reason.

The Safe Harbor Lists are maintained for the very purpose of allowing European businesses and consumers to verify which U.S. organizations participate in Safe Harbor. Anyone who is interested in verifying whether an organization is entitled to the benefits of Safe Harbor can do this by visiting the Safe Harbor website and focusing on several key elements. First, one can search the List(s) to see whether the U.S. organization is on the List(s); and if it is, whether its "Certification Status" is "Current" or "Not Current" (i.e., whether its "Certification Status" has lapsed). If an organization's "Certification Status" is "Current", then the next step would be to click on the link leading to the organization's individual record where one could find the location of the organization's relevant privacy policy statement, as well as the contact information of the individual(s) responsible for handling requests concerning its Safe Harbor commitments, the types of personal data covered by the self-certification, and a description of the organization's activities relating to the processing of those data. In addition, each record also indicates a third-party dispute resolution provider that will handle any complaints by affected EU/EEA and/or Swiss data subjects that were not satisfactorily addressed by the organization when first presented with the complaints. If any questions arise during such a review of a given organization's record, one could contact the U.S. organization itself and/or the ITA's Safe Harbor Team.

The ITA agrees that verification by European businesses of U.S. organizations' participation in Safe Harbor is a good business practice. Businesses should document when they have verified a given organization's active participation in Safe Harbor, so that they could provide such documentation to data protection authorities if and when evidence of verification is requested.

The ITA has, in the interests of transparency, clarified the guidance that it provides to prospective and current participants concerning how to meet the requirements set forth in the Framework(s). This guidance provides, inter alia, that if an organization (1) has a public website on which it has posted a general privacy policy statement or made any other representation regarding its privacy practices; and (2) has chosen to cover personal data (e.g., client or customer data) other than its own human resources data under its self-certification, then it must include in the posted privacy policy statement an affirmative statement that it complies with and has self-certified its adherence to Safe Harbor. Aside from clarifying that in the vast majority of circumstances (i.e., unless the privacy policy exclusively covers an organization's own human resources data, in which case it need only be made available to the organization's employees and as part of the Safe Harbor review process) the privacy policy must be made readily available on an organization's public website, the ITA has also emphasized that the posted privacy-related language should also include either a hyperlink to the Safe Harbor website or the corresponding URL (e.g., http://www.export.gov/safeharbor/), as well as appropriate contact information for the relevant third-party dispute resolution provider.

The ITA Safe Harbor Team diligently reviews the self-certification and recertification submissions that it receives and takes great care in maintaining the accuracy of the Safe Harbor List(s). It is incumbent upon European businesses and consumers to check the Safe Harbor List(s) to verify an organization's Safe Harbor claims and the status of its certification. The Safe Harbor List(s) should be checked, at a minimum, any time a privacy concern arises or before a contract is entered into or renewed with an organization claiming active participation in Safe Harbor.

Any misrepresentation to the general public concerning an organization's adherence to the Safe Harbor Privacy Principles may be actionable by the relevant government body (n.b., in most cases this will be the U.S. Federal Trade Commission (FTC)); therefore, allegations that an organization is making or has made false claims as to its participation in Safe Harbor should be brought to the attention of the ITA, as well as the FTC.

Although it is true that Safe Harbor operates as an enforceable self-certification program, it is also true that the ITA plays an important oversight role.

The ITA's Safe Harbor Team reviews every Safe Harbor self-certification and annual re-certification submission that it receives to ensure that these include all of the elements required by the Framework(s) (i.e., all submissions must be reviewed before they can be finalized)[2]. When an organization's Safe Harbor submission falls short the ITA contacts the organization to explain what is lacking and what steps must be taken before the organization's initial self-certification or re-certification may be finalized.

If the organization fails to rectify the issue(s) identified, the ITA does not finalize its initial self-certification or re-certification. In the case of an initial self-certification submission, the organization will never appear on the public Safe Harbor List(s). In the case of a re-certification submission, the organization's "Certification Status" is re-designated as "Not Current" in its record on the public Safe Harbor List(s) and the ITA notifies the organization's "Organization Contact" that its Safe Harbor certification has lapsed.

[2] *See*, U.S. Department of Commerce Safe Harbor Certification Review Process. Available at: http://export.gov/static/Safe%20Harbor%20Certification%20Review%20Process%20Overview_FINAL_updated%2003-08-2013_Latest_eg_main_062420.pdf

Each review includes a determination as to whether the organization in question is using the U.S.-EU Safe Harbor Framework certification mark, and if so, whether it is doing so in accordance with the specific set of instructions. Each organization that is found to be misusing the certification mark in any way is notified of its obligation to correct the use of the mark immediately and warned that failure to comply with the instructions may result in enforcement of the mark through an action for infringement of the mark, and/or a referral to the FTC for investigation of an unfair or deceptive trade practice under section 5 of the Federal Trade Commission Act.

For example, during the first nine months of 2013, the ITA notified approximately 56% of the organizations from which it had received first-time self-certification submissions and 27% of the organizations from which it had received recertification submissions to inform the organizations of shortcomings identified during the review. Over the same period, approximately 12% of the organizations from which the ITA had received first-time self-certification submissions never made it on the Safe Harbor List(s), because they did not comply with the Safe Harbor standards for self-certification.

Safe Harbor requires that there be "readily available and affordable" dispute resolution.

Approximately 80% of Safe Harbor organizations have chosen a dispute resolution provider that is entirely free to consumers (i.e., affected data subjects). The remaining organizations have chosen providers that charge a maximum of $200-250 to consumers, a cost which the Safe Harbor participant can elect to cover. Any costs above that amount are paid by the Safe Harbor participant.

The dispute resolution process offers several phases in which a data subject may have his or her complaint resolved, and the overwhelming majority of complaints and disputes are resolved at either the first or second phase. A data subject should first communicate his/her complaint/concern to the relevant Safe Harbor participant (i.e., a U.S. organization that appears on the Safe Harbor List(s)). If the data subject does not receive a timely or otherwise satisfactory response from the Safe Harbor participant, the issue can be escalated to the appropriate third party dispute resolution provider that the Safe Harbor participant has identified in its self-certification (i.e., which can be accessed on the public Safe Harbor List(s)) as being empowered to investigate unresolved complaints. If the Safe Harbor participant refuses to comply with the dispute resolution provider's findings and/or recommendations, the issue can be referred to the attention of the FTC or, if the organization is an air carrier or ticket agent, the U.S. Department of Transportation (n.b., the ITA should be informed as well).

The U.S. Federal Trade Commission (FTC) has brought ten Safe Harbor-related enforcement actions, which resulted in consent decrees that are protecting hundreds of millions of citizens in Europe and the United States.

To date the FTC has brought ten Safe Harbor-related enforcement actions, resulting in consent decrees protecting individuals worldwide. These consent decrees can be and have been enforced with significant civil penalties. For example, one organization recently agreed to a $22.5 million settlement. The FTC has always committed to prioritize referrals from EU and Swiss data protection authorities, as well as private sector third-party dispute resolution providers; however, the FTC can and has pursued cases on

its own initiative[3]. Moreover, the FTC has recently announced that Safe Harbor-related investigations are ongoing[4].

ITA's Safe Harbor Team can be reached at Safe.Harbor@trade.gov to answer any questions regarding the Safe Harbor program.

[3] *See*, summary prepared by the Safe Harbor Team of FTC enforcement of Safe Harbor-related commitments. Available at: http://export.gov/build/groups/public/@eg_main/@safeharbor/documents/webcontent/eg_main_052211.pdf. Please note that the FTC updated the Safe Harbor material on its own website (see http://business.ftc.gov/us-eu-safe-harbor-framework) in late 2012 to include detailed information regarding such enforcement (see http://business.ftc.gov/legal-resources/2840/35).
[4] *See* speech by Chairwoman Ramirez. Available at: http://www.ftc.gov/speeches/ramirez/131029tacdremarks.pdf (page 8). *See* also speech by Commissioner Brill. Available at: http://www.ftc.gov/speeches/brill/131029europeaninstituteremarks.pdf (page 6).