Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing

These questions and answers were developed by the U.S. Department of Commerce's International Trade Administration (ITA) to provide some clarification regarding the U.S.-EU Safe Harbor Framework and how the Framework applies to cloud computing. This clarification was prepared, in part, to respond to inquiries generated by the July 2012 Article 29 Working Party Opinion on Cloud Computing, as well as an opinion and various statements made by certain EU Member State data protection authorities. ITA does not believe that "cloud computing" represents an entirely new business model or presents any unique issues for Safe Harbor. The existing Safe Harbor Privacy Principles are comprehensive and flexible enough to address the issues raised by the cloud computing model; nevertheless, ITA offers the following information as guidance, given that organizations and authorities continue to grapple with how best to apply data protection principles to the cloud environment.

General Background on Cloud Computing

- "Cloud computing" is not a radically new concept, but is instead a term that was developed to explain, as well as market, the shift towards a utility model of decentralized computing. Businesses and governments have long used centralized data storage and processing; however, advancements in broadband Internet access, processor speeds, data storage, virtualization, and mobile computing technologies have made it more cost-effective to shift the burdens associated with acquiring and maintaining computing resources to off-site providers. This shift encompasses five traits: (1) consumer-initiated and on-demand; (2) broad network access (e.g., broadband and 3G/4G wireless); (3) resource pooling (i.e., ability for multiple users to share resources); (4) elasticity (i.e., rapid reallocation and provisioning of resources, such as memory); and (5) measured service (i.e., ability to abstract and sell services in terms of units of time and data used). [1] In short, cloud computing refers to the use of computing resources (i.e., hardware and software), which are delivered as a service over a network, typically the Internet.

General Background on the Role of the U.S.-EU Safe Harbor Framework

- Under the European Union (EU) 1995 Data Protection Directive (hereinafter the Directive) and the Member State laws that implement the Directive, personal data that is or will be processed may only be transferred to a country outside of the EU/EEA if that country has been formally recognized by the EU as ensuring an "adequate level of protection"[2]. The Directive, which defines the terms *personal data*[3] and *processing*[4] quite broadly,

[1] *See*, the Definition of Cloud Computing issued by the National Institute of Standards and Technology (NIST), U.S. Department of Commerce: "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Available at: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf N.b., cloud computing encompasses three service models (i.e., Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS)) and four deployment models (i.e., Private Cloud, Community Cloud, Public Cloud, and Hybrid Cloud).

[2] Directive 95/46/EC, CHAPTER IV TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES Article 25(1): "The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection." N.b., certain exemptions to the general prohibition exist, such as when the express permission of a data subject has been obtained or when the transfer is necessary for the execution of an agreement. *See* Directive 95/46/EC, CHAPTER IV TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES Article 26. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

applies to most activities involving the collection, use, and storage of personal information. The U.S. data protection framework has not been recognized by the EU as one that ensures "adequate" data protection, stemming in part from the fact that it is based on a combination of sector-specific privacy legislation and self-regulation rather than general, overarching legislation along the lines of the Directive and relevant Member State laws. In order to bridge this gap, the U.S. Department of Commerce (hereinafter the DOC) and the European Commission (hereinafter the Commission) developed the U.S.-EU Safe Harbor Framework, which the Commission formally determined in 2000 ensures "adequate" data protection. The European Economic Area (EEA) also has recognized[5] the U.S.-EU Safe Harbor Framework as ensuring "adequate" data protection. The U.S.-EU Safe Harbor Framework and the Commission's "adequacy" finding, which is binding on all EU Member States, establish that the benefits of the "safe harbor" are available only to eligible U.S. organizations that affirmatively commit themselves to adhere to the Safe Harbor Privacy Principles.

Is the U.S.-EU Safe Harbor (hereinafter Safe Harbor) applicable to cloud service provider agreements?

- Yes, Safe Harbor[6] and the Commission's "adequacy" decision[7] apply to such agreements that involve the transfer of *personal data*[8] from the EU to organizations established in the United States.

Is a cloud service provider required to enter into a contract even if it is Safe Harbor-compliant and is receiving personal data merely for processing?

- Yes, the Directive explicitly requires that all data controllers[9] in the EU (1) confirm that the data processor[10] – irrespective of where it is located – provides sufficient data protection guarantees (i.e. technical security and

---

[3] Directive 95/46/EC, CHAPTER I GENERAL PROVISIONS Article 2(a): "'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;"

[4] Directive 95/46/EC, CHAPTER I GENERAL PROVISIONS Article 2(b): "'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;"

[5] *See*, EEA Joint Committee Decision No. 108/2000 of November 30, 2000 available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:045:0047:0048:EN:PDF. The Agreement on the European Economic Area (EEA), brings together the EU Member States and three EFTA countries — Iceland, Liechtenstein and Norway — in a single internal market. Switzerland, which is an EFTA country, is not part of the EEA Agreement, but has a bilateral agreement with the EU. The EEA Agreement provides for the inclusion of EU legislation covering the four freedoms — the free movement of goods, services, persons and capital — throughout the EEA Member States. In addition, the Agreement covers cooperation in other important areas, such as consumer protection.

[6] U.S.-EU Safe Harbor Privacy Principles, issued by the U.S. Department of Commerce on July 21, 2000, provide in part: "Organizations may wish for practical or other reasons to apply the Principles to all their data processing operations, but they are only obligated to apply them to data transferred after they enter the safe harbor." Available at: http://export.gov/safeharbor/eu/eg_main_018475.asp

[7] The Safe Harbor "adequacy" decision issued by the European Commission in 2000 provides in part in Article 1: "For the purposes of Article 25(2) of Directive 95/46/EC, for all the activities falling within the scope of that Directive, the "Safe Harbor Privacy Principles" (hereinafter "the Principles"), as set out in Annex I to this Decision, implemented in accordance with the guidance provided by the Frequently Asked Questions (hereinafter "the FAQs") issued by the US Department of Commerce on 21.07.2000 as set out in Annex II to this Decision are considered to ensure an adequate level of protection for personal data transferred from the Community to organizations established in the United States"; and in Article 5: "Member States shall take all the measures necessary to comply with this Decision […]". Available at: http://export.gov/static/sh_en_DecisionSECGEN-EN_Latest_eg_main_018400.pdf

[8] U.S.-EU Safe Harbor Privacy Principles, issued by the U.S. Department of Commerce in 2000, provide in part: "'Personal data' and 'personal information' are data about an identified or identifiable individual that are within the scope of the Directive, received by a U.S. organization from the European Union, and recorded in any form. " Available at: http://export.gov/safeharbor/eu/eg_main_018475.asp

organizational measures) and (2) conclude a contract providing that the data processor shall act only on behalf of and pursuant to the instructions from the data controller and in compliance with all data security requirements that apply to the data controller[11].

- Safe Harbor fully acknowledges this requirement, explaining that the purpose of the contract is to protect the interests of the data controller who retains full responsibility for the data vis-à-vis the data subject(s) concerned[12].

- One of the principal advantages of Safe Harbor certification is that: "contracts with Safe Harbor participants for mere processing" (i.e., contracts between EU data controllers and U.S. data processors) do not require prior authorization or such authorization will be granted automatically by the Member States[13], whereas contracts with recipients not participating in the Safe Harbor or otherwise not providing "adequate" protection may require prior authorization by relevant data protection authorities.

Does Safe Harbor require that the contract incorporate the standard contractual clauses adopted by the Commission?

- No, when it comes to mere processing of data, the EU standard contractual clauses represent an alternative to Safe Harbor certification, not an additional requirement (i.e., either option would allow a service provider to ensure an "adequate" level of data protection).

- In short, when drafting contractual clauses concerning data transfers for mere processing where the service provider is Safe Harbor-compliant the parties are free to draft their own agreement, use templates promulgated by individual Member States or use the EU standard contractual clauses.

Has the Commission issued any new requirements regarding Safe Harbor that would reduce the value of certification to cloud service providers?

- No, neither Safe Harbor nor the Commission's "adequacy" decision has been amended.

- Although the Article 29 Working Party (hereinafter Art. 29 WP) adopted an opinion on cloud computing in July 2012, which featured a variety of recommendations including ones relevant to international transfers, that

---

[9] Directive 95/46/EC, CHAPTER I GENERAL PROVISIONS Article 2(d): 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;"

[10] Directive 95/46/EC, CHAPTER I GENERAL PROVISIONS Article 2(e): "'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;"

[11] *See*, Directive 95/46/EC, CHAPTER II GENERAL RULES ON THE LAWFULNESS OF THE PROCESSING OF PERSONAL DATA, SECTION VIII CONFIDENTIALITY AND SECURITY OF PROCESSING, Article 17. N.b., a data controller must always comply with the requirements of local data protection laws (e.g., notifications to data protection authorities and data subjects, appointment of data protection officers, minimization of data collection, usage, and retention, data security, etc.).

[12] The U.S.-EU Safe Harbor FAQ 10: Article 17 Contracts, which was issued with other Frequently Asked Questions and Answers (FAQs) by the U.S. Department of Commerce in 2000 along with the U.S.-EU Safe Harbor Privacy Principles, provides in part: "Data controllers in the European Union are always required to enter into a contract when a transfer for mere processing is made, whether the processing operation is carried out inside or outside of the EU. The purpose of the contract is to protect the interests of the data controller, i.e., the person or body who determines the purposes and means of processing, who retains full responsibility for the data *vis-à-vis* the individuals concerned. The contract thus specifies the processing to be carried out and any measures necessary to ensure that the data are kept secure." Available at: http://export.gov/safeharbor/eu/eg_main_018382.asp

[13] *Ibid.,* U.S.-EU Safe Harbor FAQ 10: Article 17 Contracts, also provides in part: "Because adequate protection is provided by Safe Harbor participants, contracts with Safe Harbor participants for mere processing do not require prior authorization (or such authorization will be granted automatically by the Member States) as would be required for contracts with recipients not participating in the Safe Harbor or otherwise not providing adequate protection."

opinion is nonbinding[14]. The opinions, working documents, letters, etc. issued by the Art. 29 WP are advisory in nature[15]. The Art. 29 WP's views and recommendations should not be attributed to the Commission, and are not binding on either the Commission itself or the Member States.

- Even though the Art. 29 WP opinion on cloud computing is nonbinding, it is worth examining what was said with regard to Safe Harbor, as the opinion has received a certain amount of attention:
    - The discussion on Safe Harbor begins with the general observation that "Adequacy findings, including Safe Harbor, are limited in respect of the geographical scope, and therefore do not cover all transfers within the Cloud."[16] , but follows this with a repetition of the official Commission position that "[T]ransfers to US organizations adhering to the principles can take place lawfully under EU law since the recipient organizations are deemed to provide an adequate level of data protection to the transferred data."[17]
        - Safe Harbor does provide for the possibility that data originally transferred to a Safe Harbor-compliant data processor could in turn be transferred by said processor to a sub-processor located in another country. A Safe Harbor-compliant data processor can transfer data to a sub-processor in a country that has not been recognized as ensuring "adequate" data protection, provided that the processor and sub-processor enter into a written agreement requiring that the sub-processor provide at least the same level of data protection to the data as is required by the relevant Safe Harbor Privacy Principles. [18]
    - The Art. 29 WP 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."[19] (emphasis added). The opinion clarifies that it "considers that companies exporting data should not merely rely on the statement of the data importer claiming that he has a Safe Harbor certification", but should instead "obtain evidence that the Safe Harbor self-certifications [*sic*] exists and request evidence demonstrating that their principles are complied with." [20] (emphasis added).
        - The DOC maintains a public list[21] featuring the Safe Harbor records of organizations that have self-certified their compliance with Safe Harbor (n.b., the records include, amongst other things,

[14] Art. 29 WP, Opinion 5/2012 on Cloud Computing of July 1, 2012, PP 17-27. Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

[15] *See*, the European Commission website at http://ec.europa.eu/justice/data-protection/article-29/index_en.htm

[16] Art. 29 WP, Opinion 5/2012 on Cloud Computing of July 1, 2012, P 17.

[17] *Ibid.*

[18] The U.S.-EU Safe Harbor Privacy Principles issued by the U.S. Department of Commerce in 2000 provide in part: "**ONWARD TRANSFER:** To disclose information to a third party, organizations must apply the Notice and Choice Principles. Where an organization wishes to transfer information to a third party that is acting as an agent […] it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles. If the organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing." (http://export.gov/safeharbor/eu/eg_main_018475.asp)

[19] *Ibid.*

[20] *Ibid.*

[21] The DOC maintains a list of organizations that self-certify their adherence to the Safe Harbor Privacy Principles in accordance with the guidance set forth in FAQ 6: Self-Certification, and updates this list on the basis of annual "letters and notifications" received pursuant to FAQ 11: Dispute Resolution and Enforcement. Organizations should provide such self-certification submissions to the DOC not less than annually; otherwise, they will be removed from the list of "Current" Safe

the locations of the organizations' privacy policies, the independent recourse mechanism(s) available to investigate unresolved complaints, their method of verification, the categories of data covered, and organization contact information); therefore, EU data controllers can easily and authoritatively verify whether a given U.S. data processor appears on the Safe Harbor List and whether the latter's certification status is "Current" or "Not Current".

- The Art. 29 WP opinion states that a cloud client "must verify if the standard contracts composed by cloud providers are compliant with national requirements regarding contractual data processing"[22], and considers that "commitment to Safe Harbor cannot substitute"[23] for the lack of specified guarantees (e.g., identification of the location of sub-processors) when such guarantees are required by national legislation. Where a given cloud provider's standard contract does not provide such guarantees, the client is "encouraged to use other legal instruments available, such as [EU] standard contractual clauses"[24] (emphasis added).

  - A data controller subject to the Directive or Member State laws implementing the Directive must comply with the data protection requirements set forth therein[25]; however, it is an eligible U.S. organization's voluntary, but fully enforceable commitment to adhere to the Safe Harbor Privacy Principles (i.e., supported by independent dispute resolution and subject to enforcement by the Federal Trade Commission[26]) that provides the guarantee of "adequate" protection under Safe Harbor. Additional requirements cannot be imposed exclusively on U.S. service providers processing personal data transferred from the EU simply because they satisfy the "adequacy" requirement through Safe Harbor certification (i.e., the same basic rules apply to all

---

Harbor records and Safe Harbor benefits will no longer be assured. Both the list and the self-certification submissions are made publicly available on the Safe Harbor website (see https://safeharbor.export.gov/list.aspx). All organizations that self-certify for the Safe Harbor must also state in their relevant published privacy policy statements that they adhere to the Principles. An organization must 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. An organization does not need to subject all personal information to the Principles, but it must subject to the Principles all personal data received from the EU after it joins the Safe Harbor. Any misrepresentation to the general public concerning an organization's adherence to the Principles may be actionable by the Federal Trade Commission (FTC) or other relevant government body. Misrepresentations to the DOC may be actionable under the False Statements Act (18 U.S.C. § 1001). *See*, the U.S.-EU Safe Harbor FAQ 6: Self-Certification, which was issued with other Frequently Asked Questions and Answers (FAQs) by the U.S. Department of Commerce in 2000 along with the U.S.-EU Safe Harbor Privacy Principles. Available at: http://export.gov/safeharbor/eu/eg_main_018388.asp. *See*, also the U.S.-EU Safe Harbor Privacy Principles issued by the U.S. Department of Commerce in 2000, which provide in part: "Safe Harbor benefits are assured from the date on which each organization wishing to qualify for the Safe Harbor self-certifies to the Department of Commerce (or its designee) its adherence to the Principles in accordance with the guidance set forth in the Frequently Asked Question on Self-Certification." Available at: http://export.gov/safeharbor/eu/eg_main_018475.asp

[22] Art. 29 WP, Opinion 5/2012 on Cloud Computing of July 1, 2012, P 17.

[23] Art. 29 WP, Opinion 5/2012 on Cloud Computing of July 1, 2012, P 18.

[24] *Ibid.*

[25] *See*, the U.S.-EU Safe Harbor Privacy Principles issued by the U.S. Department of Commerce in 2000, which provide in part: "The Principles […] are intended for use solely by U.S. organizations receiving personal data from the European Union for the purpose of qualifying for the safe harbor and the presumption of "adequacy" it creates. Because the Principles were solely designed to serve this specific purpose, their adoption for other purposes may be inappropriate. The Principles cannot be used as a substitute for national provisions implementing the Directive that apply to the processing of personal data in the Member States." Available at: http://export.gov/safeharbor/eu/eg_main_018475.asp

[26] The U.S.-EU Safe Harbor FAQ 11: Dispute Resolution and Enforcement, which was issued with other Frequently Asked Questions and Answers (FAQs) by the U.S. Department of Commerce in 2000 along with the U.S.-EU Safe Harbor Privacy Principles, provides in part: "**FTC Action:** The FTC has committed to reviewing on a priority basis referrals received from privacy self-regulatory organizations […] and EU Member States alleging non-compliance with the Safe Harbor Principles to determine whether Section 5 of the FTC Act prohibiting unfair or deceptive acts or practices in commerce has been violated. If the FTC concludes that it has reason[s] to believe Section 5 has been violated, it may resolve the matter by seeking an administrative cease and desist order prohibiting the challenged practices or by filing a complaint in a federal district court, which if successful could result in a federal court order to same effect. The FTC may obtain civil penalties for violations of an administrative cease and desist order and may pursue civil or criminal contempt for violation of a federal court order." Available at: http://export.gov/safeharbor/eu/eg_main_018383.asp. *See*, also, Safe Harbor Enforcement Overview available at: http://export.gov/safeharbor/eu/eg_main_018481.asp

cloud service providers whether they be located in the EU or an "adequate" country, or Safe Harbor-compliant).

- Finally, the Art. 29 WP states that "the Safe Harbor principles by themselves may also not guarantee the data exporter the necessary means to ensure that appropriate security measures have been applied by the cloud provider in the US, as may be required by national legislations [*sic*] based on the Directive 95/46/EC"[27], as "cloud computing raises several cloud-specific security risks, such as loss of governance, insecure or incomplete data deletion, insufficient audit trails or isolation failures, which are not sufficiently addressed by the existing Safe Harbor principles on data security."[28] Art. 29 WP concludes that "it might be advisable to complement the commitment of the data importer to the Safe Harbor with additional safeguards taking into account the specific nature of the cloud."[29] (emphasis added).

  - Safe Harbor is a principles-based framework; therefore, the Security Principle[30] leaves to the data controller and data processor to define the specific security requirements in the contract. Safe Harbor's requirement that "reasonable precautions"[31] be taken echoes the requirement set forth in the Directive[32] that the data controller "implement appropriate technical and organizational measures to protect personal data"[33], which often entails the obligation to ensure that it choose a "processor providing sufficient guarantees in respect of the technical and security measures and organizations measures governing the processing to be carried out"[34] and that the latter complies with those measures.

May Member State data protection authorities unilaterally refuse to recognize Safe Harbor certification as a valid means of demonstrating that a service provider ensures an adequate level of data protection?

- No, the Commission's Safe Harbor adequacy decision is binding on all EU Member States[35] and by extension all EEA Member States[36].

---

[27] Art. 29 WP, Opinion 5/2012 on Cloud Computing of July 1, 2012, P 18.

[28] *Ibid.*

[29] *Ibid.*

[30] The U.S.-EU Safe Harbor Privacy Principles issued by the U.S. Department of Commerce in 2000 provide in part: "**SECURITY:** Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction." Available at: http://export.gov/safeharbor/eu/eg_main_018475.asp

[31] *Ibid.*

[32] *See*, Directive 95/46/EC, CHAPTER II GENERAL RULES ON THE LAWFULNESS OF THE PROCESSING OF PERSONAL DATA, SECTION VIII CONFIDENTIALITY AND SECURITY OF PROCESSING, Article 17.

[33] *Ibid.*, Article 17(1).

[34] *Ibid.*, Article 17(2).

[35] The Safe Harbor "adequacy" decision issued by the European Commission in 2000, *Article 1* provides in part: "For the purposes of Article 25(2) of Directive 95/46/EC, for all the activities falling within the scope of that Directive, the "Safe Harbor Privacy Principles" […] implemented in accordance with the guidance provided by the Frequently Asked Questions […] issued by the US Department of Commerce on 21.07.2000 […] are considered to ensure an adequate level of protection for personal data transferred from the Community to organizations established in the United States" and Article 5 clarifies: "Member States shall take all the measures necessary to comply with this Decision at the latest at the end of a period of ninety days from the date of its notification to the Member States." Available at: http://export.gov/static/sh_en_DecisionSECGEN-EN_Latest_eg_main_018400.pdf

[36] See the EEA Joint Committee Decision of November 30, 2000, amending Annex XI (Telecommunication services) to the EEA Agreement, incorporating by reference the 2000/520/EC Commission Decision of July 26, 2000.

What will happen to Safe Harbor while the EU proceeds with its deliberations concerning the proposal to replace the existing Directive?

- Compliance with Safe Harbor will remain an officially recognized means of demonstrating that an eligible U.S. organization ensures an adequate level of data protection while the EU data protection reform proceeds.

- Over the past year, both U.S. and EU officials have expressed their continued commitment to Safe Harbor. The DOC and the Commission publicly reaffirmed their commitment to Safe Harbor when they issued a joint statement in March 2012[37]. On the margins of the October 10, 2012, European Parliament Interparliamentary Committee meeting on the reform of the EU data protection framework, European Commission Vice President Viviane Reding noted that "Nothing will change on this. Safe Harbor will stay." Paul Nemitz, Director for Fundamental Rights and Citizenship within the European Commission's Justice Directorate General, also made several positive comments regarding Safe Harbor during this meeting, noting amongst other points that "there is more confidence in Safe Harbor" and that "the trend is positive"[38].

- The relevant EU institutions are currently debating a proposal to replace the existing Directive with a "General Data Protection Regulation"[39] (hereinafter the Proposed Regulation), but the Directive will remain in force until a new law is passed and enters into force. The Commission's draft of the Proposed Regulation expressly states that existing "adequacy" findings would be recognized, which would mean that Safe Harbor would continue to offer eligible U.S. organizations an accepted means of demonstrating "adequacy." In January 2013, the rapporteur to the Civil Liberties, Justice and Home Affairs (LIBE) Committee of the European Parliament presented the Committee with a report consolidating and distilling thousands of amendments to the Proposed Regulation. One of the amendments featured in the report would place a two-year sunset on all existing "adequacy" findings, including the Safe Harbor finding[40]. Even if this amendment were to be adopted in the final version of the Proposed Regulation, it would not enter into effect until two years after the Regulation is finalized (i.e., 2016 at the earliest). It is important to note that the LIBE report was made for one committee of one of the three EU institutions (i.e., the Commission, the European Parliament, and the Council of the European Union); therefore, the changes suggested therein are by no means final. In short, the Proposed Regulation is likely to change significantly as it moves through the legislative process. The DOC will continue to monitor the Proposed Regulation and will inform Safe Harbor organizations should the final law affect the operation of Safe Harbor.

How should a cloud service provider respond when concerns about the U.S. Patriot Act are raised by prospective or existing EU customers?

---

[37] U.S.-EU Joint Statement on Privacy from EU Commission Vice-President Viviane Reding and U.S. Commerce Secretary John Bryson, March 19, 2012. The Joint Statement provided in part that "In line with the objectives of increasing trade and regulatory cooperation outlined by our leaders at the U.S.-EU Summit, the United States and the European Union reaffirm their respective commitments to the U.S.-EU Safe Harbor Framework." Available at: http://www.commerce.gov/news/press-releases/2012/03/19/us-eu-joint-statement-privacy-eu-commission-vice-president-viviane-re

[38] *See*, Interparliamentary meeting on Data Protection SESSION VII - Data Protection in the global context (16:17). Available at: http://www.europarl.europa.eu/ep-live/en/committees/video?event=20121010-1500-COMMITTEE-LIBE&category=COMMITTEE&format=wmv

[39] 2012/0011 (COD) Proposal for a General Data Protection Regulation, CHAPTER V - TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS, Article 41(8): "Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force, until amended, replaced or repealed by the Commission." Available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[40] See, DRAFT REPORT on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) Committee on Civil Liberties, Justice and Home Affairs Rapporteur: Jan Philipp Albrecht, Amendment 75, Recital 134. Available at http://www.huntonprivacyblog.com/wp-content/uploads/2013/01/Albrecht-Report-LIBE.pdf

- On December 4, 2012, the U.S. Ambassador to the EU, William Kennard, presented remarks before Forum Europe's 3rd Annual European Data Protection and Privacy Conference.

- During these remarks, Ambassador Kennard noted that "the transatlantic privacy discussion is too often sidetracked by misconceptions about the U.S. legal system – myths that obscure our fundamental commitment to privacy and the extensive legal protections we provide to date"[41].

These misconceptions are addressed in a paper, which is publicly available via the website noted below, entitled "Five Myths Regarding Privacy and Law Enforcement Access to Personal Information in the European Union and the United States"[42]. The paper is intended to clarify these issues and should prove useful when concerns are raised.

Conclusion:

ITA offers this guidance to clarify that Safe Harbor continues to offer eligible U.S. organizations, regardless of whether or not they are operating in the cloud environment, an officially recognized means of complying with the Directive's "adequacy" requirement. ITA invites organizations or individuals with questions about these or other issues concerning Safe Harbor's operation to contact ITA's Safe Harbor Team at safe.harbor@trade.gov.

[41] *See*, http://useu.usmission.gov/kennard_120412.html

[42] *See*, http://photos.state.gov/libraries/useu/231771/PDFs/Five%20Myths%20Regarding%20Privacy%20and%20Law%20Enforcement_October%209_2012_pdf.pdf