ANNEX I

UNITED STATES DEPARTMENT OF COMMERCE
The Secretary of Commerce
Washington, D.C. 20230

February 23, 2016

Ms. Věra Jourová
Commissioner for Justice, Consumers
and Gender Equality
European Commission
Rue de la Loi / Wetstraat 200
1049 Brussels
Belgium

Dear Commissioner Jourová:

On behalf of the United States, I am pleased to transmit herewith a package of EU-U.S. Privacy Shield materials that is the product of two years of productive discussions among our teams. This package, along with other materials available to the Commission from public sources, provides a very strong basis for a new adequacy finding by the European Commission.

We should both be proud of the improvements to the Framework. The Privacy Shield is based on Principles that have strong consensus support on both sides of the Atlantic, and we have strengthened their operation. Through our work together, we have the real opportunity to improve the protection of privacy around the world.

The Privacy Shield Package includes the Privacy Shield Principles, along with a letter, attached as Annex 1, from the International Trade Administration (ITA) of the Department of Commerce, which administers the program, describing the commitments that our Department has made to ensure that the Privacy Shield operates effectively. The Package also includes Annex 2, which includes other Department of Commerce commitments relating to the new arbitral model available under the Privacy Shield.

I have directed my staff to devote all necessary resources to implement the Privacy Shield Framework expeditiously and fully and to ensure the commitments in Annex 1 and Annex 2 are met in a timely fashion.

The Privacy Shield Package also includes other documents from other United States agencies, namely:

- A letter from the Federal Trade Commission (FTC) describing its enforcement of the Privacy Shield;
- A letter from the Department of Transportation describing its enforcement of the Privacy Shield;

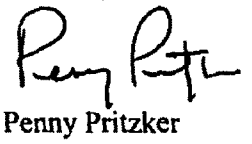
- A letter prepared by the Office of the Director of National Intelligence (ODNI) regarding safeguards and limitations applicable to U.S. national security authorities;
- A letter from the Department of State and accompanying memorandum describing the State Department's commitment to establish a new Privacy Shield Ombudsperson for submission of inquiries regarding the United States' signals intelligence practices; and
- A letter prepared by the Department of Justice regarding safeguards and limitations on U.S. Government access for law enforcement and public interest purposes.

You can be assured that the United States takes these commitments seriously.

Within 30 days of final approval of the adequacy determination, the full Privacy Shield Package will be delivered to the *Federal Register* for publication.

We look forward to working with you as the Privacy Shield is implemented and as we embark on the next phase of this process together.

Sincerely,



Penny Pritzker

FEB 2 3 2016

UNITED STATES DEPARTMENT OF COMMERCE
The Under Secretary for International Trade
Washington, D.C. 20230

The Honorable Věra Jourová
Commissioner for Justice, Consumers and Gender Equality
European Commission
Rue de la Loi/Westraat 200
1049 Brussels
Belgium

Dear Commissioner Jourová:

On behalf of the International Trade Administration, I am pleased to describe the enhanced protection of personal data that the EU-U.S. Privacy Shield Framework ("Privacy Shield" or "Framework") provides and the commitments the Department of Commerce ("Department") has made to ensure that the Privacy Shield operates effectively. Finalizing this historic arrangement is a major achievement for privacy and for businesses on both sides of the Atlantic. It offers confidence to EU individuals that their data will be protected and that they will have legal remedies to address any concerns. It offers certainty that will help grow the transatlantic economy by ensuring that thousands of European and American businesses can continue to invest and do business across our borders. The Privacy Shield is the result of over two years of hard work and collaboration with you, our colleagues in the European Commission ("Commission"). We look forward to continuing to work with the Commission to ensure that the Privacy Shield functions as intended.

We have worked with the Commission to develop the Privacy Shield to allow organizations established in the United States to meet the adequacy requirements for data protection under EU law. The new Framework will yield several significant benefits for both individuals and businesses. First, it provides an important set of privacy protections for the data of EU individuals. It requires participating U.S. organizations to develop a conforming privacy policy, publicly commit to comply with the Privacy Shield Principles so that the commitment becomes enforceable under U.S. law, annually re-certify their compliance to the Department, provide free independent dispute resolution to EU individuals, and be subject to the authority of the U.S. Federal Trade Commission ("FTC"), Department of Transportation ("DOT"), or another enforcement agency. Second, the Privacy Shield will enable thousands of companies in the United States and subsidiaries of European companies in the United States to receive personal data from the European Union to facilitate data flows that support transatlantic trade. The transatlantic economic relationship is already the world's largest, accounting for half of global economic output and nearly one trillion dollars in goods and services trade, supporting millions of jobs on both sides of the Atlantic. Businesses that rely on transatlantic data flows come from all industry sectors and include major Fortune 500 firms as well as many small and medium-sized enterprises (SMEs). Transatlantic data flows allow U.S. organizations to process data required to offer goods, services, and employment opportunities to European individuals. The Privacy Shield supports shared privacy principles, bridging the differences in our legal approaches, while furthering trade and economic objectives of both Europe and the United States.

INTERNATIONAL TRADE ADMINISTRATION

While a company's decision to self-certify to this new Framework will be voluntary, once a company publicly commits to the Privacy Shield, its commitment is enforceable under U.S. law by either the Federal Trade Commission or Department of Transportation, depending on which authority has jurisdiction over the Privacy Shield organization.

Enhancements under the Privacy Shield Principles

The resulting Privacy Shield strengthens the protection of privacy by:

- requiring additional information be provided to individuals in the Notice Principle, including a declaration of the organization's participation in the Privacy Shield, a statement of the individual's right to access personal data, and the identification of the relevant independent dispute resolution body;
- strengthening protection of personal data that is transferred from a Privacy Shield organization to a third party controller by requiring the parties to enter into a contract that provides that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles;
- strengthening protection of personal data that is transferred from a Privacy Shield organization to a third party agent, including by requiring a Privacy Shield organization to: take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles; upon notice, take reasonable and appropriate steps to stop and remediate unauthorized processing; and provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request;
- providing that a Privacy Shield organization is responsible for the processing of personal information it receives under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf, and that the Privacy Shield organization shall remain liable under the Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless the organization proves that it is not responsible for the event giving rise to the damage;
- clarifying that Privacy Shield organizations must limit personal information to the information that is relevant for the purposes of processing;
- requiring an organization to annually certify with the Department its commitment to apply the Principles to information it received while it participated in the Privacy Shield if it leaves the Privacy Shield and chooses to keep such data;
- requiring that independent recourse mechanisms be provided at no cost to the individual;
- requiring organizations and their selected independent recourse mechanisms to respond promptly to inquiries and requests by the Department for information relating to the Privacy Shield;
- requiring organizations to respond expeditiously to complaints regarding compliance with the Principles referred by EU Member State authorities through the Department; and
- requiring a Privacy Shield organization to make public any relevant Privacy Shield-related sections of any compliance or assessment report submitted to the FTC if it becomes subject to an FTC or court order based on non-compliance.

Administration and Supervision of the Privacy Shield Program by the Department of Commerce

The Department reiterates its commitment to maintain and make available to the public an authoritative list of U.S. organizations that have self-certified to the Department and declared their commitment to adhere to the Principles (the "Privacy Shield List"). The Department will keep the Privacy Shield List up to date by removing organizations when they voluntarily withdraw, fail to complete the annual re-certification in accordance with the Department's procedures, or are found to persistently fail to comply. The Department will also maintain and make available to the public an authoritative record of U.S. organizations that had previously self-certified to the Department, but that have been removed from the Privacy Shield List, including those that were removed for persistent failure to comply with the Principles. The Department will identify the reason each organization was removed.

In addition, the Department commits to strengthening the administration and supervision of the Privacy Shield. Specifically, the Department will:

Provide Additional Information on the Privacy Shield Website

- maintain the Privacy Shield List, as well as a record of those organizations that previously self-certified their adherence to the Principles, but which are no longer assured of the benefits of the Privacy Shield;
- include a prominently placed explanation clarifying that all organizations removed from the Privacy Shield List are no longer assured of the benefits of the Privacy Shield, but must nevertheless continue to apply the Principles to the personal information that they received while they participated in the Privacy Shield for as long as they retain such information; and
- provide a link to the list of Privacy Shield-related FTC cases maintained on the FTC website.

Verify Self-Certification Requirements

- prior to finalizing an organization's self-certification (or annual re-certification) and placing an organization on the Privacy Shield List, verify that the organization has:

    - provided required organization contact information;
    - described the activities of the organization with respect to personal information received from the EU;
    - indicated what personal information is covered by its self-certification;
    - if the organization has a public website, provided the web address where the privacy policy is available and the privacy policy is accessible at the web address provided, or if an organization does not have a public website, provided where the privacy policy is available for viewing by the public;
    - included in its relevant privacy policy a statement that it adheres to the Principles and if the privacy policy is available online, a hyperlink to the Department's Privacy Shield website;

- identified the specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the Principles or a future annex to the Principles);
- if the organization elects to satisfy the requirements in points (a)(i) and (a)(iii) of the Recourse, Enforcement and Liability Principle by committing to cooperate with the appropriate EU data protection authorities ("DPAs"), indicated its intention to cooperate with DPAs in the investigation and resolution of complaints brought under the Privacy Shield, notably to respond to their inquiries when EU data subjects have brought their complaints directly to their national DPAs;
- identified any privacy program in which the organization is a member;
- identified the method of verification of assuring compliance with the Principles (*e.g.*, in-house, third party);
- identified, both in its self-certification submission and in its privacy policy, the independent recourse mechanism that is available to investigate and resolve complaints;
- included in its relevant privacy policy, if the policy is available online, a hyperlink to the website or complaint submission form of the independent recourse mechanism that is available to investigate unresolved complaints; and
- if the organization has indicated that it intends to receive human resources information transferred from the EU for use in the context of the employment relationship, declared its commitment to cooperate and comply with DPAs to resolve complaints concerning its activities with regard to such data, provided the Department with a copy of its human resources privacy policy, and provided where the privacy policy is available for viewing by its affected employees.

- work with independent recourse mechanisms to verify that the organizations have in fact registered with the relevant mechanism indicated in their self-certification submissions, where such registration is required.

Expand Efforts to Follow Up with Organizations That Have Been Removed from the Privacy Shield List

- notify organizations that are removed from the Privacy Shield List for "persistent failure to comply" that they are not entitled to retain information collected under the Privacy Shield; and
- send questionnaires to organizations whose self-certifications lapse or who have voluntarily withdrawn from the Privacy Shield to verify whether the organization will return, delete, or continue to apply the Principles to the personal information that they received while they participated in the Privacy Shield, and if personal information will be retained, verify who within the organization will serve as an ongoing point of contact for Privacy Shield-related questions.

Search for and Address False Claims of Participation

- review the privacy policies of organizations that have previously participated in the Privacy Shield program, but that have been removed from the Privacy Shield List to identify any false claims of Privacy Shield participation;
- on an ongoing basis, when an organization: (a) withdraws from participation in the Privacy Shield, (b) fails to recertify its adherence to the Principles, or (c) is removed as a participant in the Privacy Shield notably for "persistent failure to comply," undertake, on an *ex officio* basis, to verify that the organization has removed from any relevant published privacy policy any references to the Privacy Shield that imply that the organization continues to actively participate in the Privacy Shield and is entitled to its benefits. Where the Department finds that such references have not been removed, the Department will warn the organization that the Department will, as appropriate, refer matters to the relevant agency for potential enforcement action if it continues to make the claim of Privacy Shield certification. If the organization neither removes the references nor self-certifies its compliance under the Privacy Shield, the Department will *ex officio* refer the matter to the FTC, DOT, or other appropriate enforcement agency or, in appropriate cases, take action to enforce the Privacy Shield certification mark;
- undertake other efforts to identify false claims of Privacy Shield participation and improper use of the Privacy Shield certification mark, including by conducting Internet searches to identify where images of the Privacy Shield certification mark are being displayed and references to Privacy Shield in organizations' privacy policies;
- promptly address any issues that we identify during our *ex officio* monitoring of false claims of participation and misuse of the certification mark, including warning organizations misrepresenting their participation in the Privacy Shield program as described above;
- take other appropriate corrective action, including pursuing any legal recourse the Department is authorized to take and referring matters to the FTC, DOT, or another appropriate enforcement agency; and
- promptly review and address complaints about false claims of participation that we receive.

The Department will undertake reviews of privacy policies of organizations to more effectively identify and address false claims of Privacy Shield participation. Specifically, the Department will review the privacy policies of organizations whose self-certification has lapsed due to their failure to re-certify adherence to the Principles. The Department will conduct this type of review to verify that such organizations have removed from any relevant published privacy policy any references that imply that the organizations continue to actively participate in the Privacy Shield. As a result of these types of reviews, we will identify organizations that have not removed such references and send those organizations a letter from the Department's Office of General Counsel warning of potential enforcement action if the references are not removed. The Department will take follow-up action to ensure that the organizations either remove the inappropriate references or re-certify their adherence to the Principles. In addition, the Department will undertake efforts to identify false claims of Privacy Shield participation by organizations that have never participated in the Privacy Shield program, and will take similar corrective action with respect to such organizations.

Conduct Periodic *ex officio* Compliance Reviews and Assessments of the Program

- on an ongoing basis, monitor effective compliance, including through sending detailed questionnaires to participating organizations, to identify issues that may warrant further follow-up action. In particular, such compliance reviews shall take place when: (a) the Department has received specific non-frivolous complaints about an organization's compliance with the Principles, (b) an organization does not respond satisfactorily to inquiries by the Department for information relating to the Privacy Shield, or (c) there is credible evidence that an organization does not comply with its commitments under the Privacy Shield. The Department shall, when appropriate, consult with the competent data protection authorities about such compliance reviews; and
- assess periodically the administration and supervision of the Privacy Shield program to ensure that monitoring efforts are appropriate to address new issues as they arise.

The Department has increased the resources that will be devoted to the administration and supervision of the Privacy Shield program, including doubling the number of staff responsible for the administration and supervision of the program. We will continue to dedicate appropriate resources to such efforts to ensure effective monitoring and administration of the program.

Tailor the Privacy Shield Website to Targeted Audiences

The Department will tailor the Privacy Shield website to focus on three target audiences: EU individuals, EU businesses, and U.S. businesses. The inclusion of material targeted directly to EU individuals and EU businesses will facilitate transparency in a number of ways. With regard to EU individuals, it will clearly explain: (1) the rights the Privacy Shield provides to EU individuals; (2) the recourse mechanisms available to EU individuals when they believe an organization has breached its commitment to comply with the Principles; and (3) how to find information pertaining to an organization's Privacy Shield self-certification. With regard to EU businesses, it will facilitate verification of: (1) whether an organization is assured of the benefits of the Privacy Shield; (2) the type of information covered by an organization's Privacy Shield self-certification; (3) the privacy policy that applies to the covered information; and (4) the method the organization uses to verify its adherence to the Principles.

Increase Cooperation with DPAs

To increase opportunities for cooperation with DPAs, the Department will establish a dedicated contact at the Department to act as a liaison with DPAs. In instances where a DPA believes that an organization is not complying with the Principles, including following a complaint from an EU individual, the DPA can reach out to the dedicated contact at the Department to refer the organization for further review. The contact will also receive referrals regarding organizations that falsely claim to participate in the Privacy Shield, despite never having self-certified their adherence to the Principles. The contact will assist DPAs seeking information related to a specific organization's self-certification or previous participation in the program, and the contact will respond to DPA inquiries regarding the implementation of specific Privacy Shield requirements. Second, the Department will provide DPAs with material

regarding the Privacy Shield for inclusion on their own websites to increase transparency for EU individuals and EU businesses. Increased awareness regarding the Privacy Shield and the rights and responsibilities it creates should facilitate the identification of issues as they arise, so that these can be appropriately addressed.

Facilitate Resolution of Complaints about Non-Compliance

The Department, through the dedicated contact, will receive complaints referred to the Department by a DPA that a Privacy Shield organization is not complying with the Principles. The Department will make its best effort to facilitate resolution of the complaint with the Privacy Shield organization. Within 90 days after receipt of the complaint, the Department will provide an update to the DPA. To facilitate the submission of such complaints, the Department will create a standard form for DPAs to submit to the Department's dedicated contact. The dedicated contact will track all referrals from DPAs received by the Department, and the Department will provide in the annual review described below a report analyzing in aggregate the complaints it receives each year.

Adopt Arbitral Procedures and Select Arbitrators in Consultation with the Commission

The Department will fulfill its commitments under Annex I and publish the procedures after agreement has been reached.

Joint Review Mechanism of the Functioning of the Privacy Shield

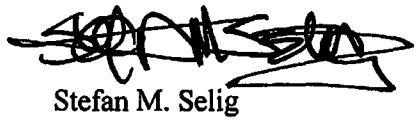
The Department of Commerce, the FTC, and other agencies, as appropriate, will hold annual meetings with the Commission, interested DPAs, and appropriate representatives from the Article 29 Working Party, where the Department will provide updates on the Privacy Shield program. The annual meetings will include discussion of current issues related to the functioning, implementation, supervision, and enforcement of the Privacy Shield, including referrals received by the Department from DPAs, the results of *ex officio* compliance reviews, and may also include discussion of relevant changes of law.

National Security Exception

With respect to the limitations to the adherence to the Privacy Shield Principles for national security purposes, the General Counsel of the Office of the Director of National Intelligence, Robert Litt, has also sent a letter addressed to Justin Antonipillai and Ted Dean of the Department of Commerce, and this has been forwarded to you. This letter extensively discusses, among other things, the policies, safeguards, and limitations that apply to signals intelligence activities conducted by the U.S. In addition, this letter describes the transparency provided by the Intelligence Community about these matters. As the Commission is assessing the Privacy Shield Framework, the information in this letter provides assurance to conclude that the Privacy Shield will operate appropriately, in accordance with the Principles therein. We understand that you may raise information that has been released publicly by the Intelligence Community, along with other information, in the future to inform the annual review of the Privacy Shield Framework.

On the basis of the Privacy Shield Principles and the accompanying letters and materials, including the Department's commitments regarding the administration and supervision of the Privacy Shield Framework, our expectation is that the Commission will determine that the EU-U.S. Privacy Shield Framework provides adequate protection for the purposes of EU law and data transfers from the European Union will continue to organizations that participate in the Privacy Shield.

Sincerely,



Stefan M. Selig