UNITED STATES DEPARTMENT OF COMMERCE
Office of the Secretary
Washington, D.C. 20230

January 9, 2017

His Excellency
Johann N. Schneider-Ammann
Federal Councillor
The Federal Department of Economic Affairs, Education
and Research
Bundeshaus Ost
3003 Bern

Dear Federal Councillor Schneider-Ammann:

On behalf of the United States, I am pleased to transmit herewith a package of Swiss-U.S. Privacy Shield materials. The Swiss-U.S. Privacy Shield reflects our shared objective of enhancing privacy protection for our citizens and reinforcing legal certainty for firms in our countries.

It is our understanding that, on the basis of this package, along with other materials available from public sources, Switzerland intends to recognize the adequacy of protection provided by the Privacy Shield Principles as meeting the requirements of Article 6 of the Swiss Federal Act on Data Protection.

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 that the commitments in Annex 1 and Annex 2 are met in a timely fashion.

The Privacy Shield Package also includes:

- 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; and

- A letter from the Department of State and accompanying memorandum describing the Department's commitment to make available to Swiss individuals a Privacy Shield Ombudsperson Mechanism for submission of inquiries regarding United States' signals intelligence practices.

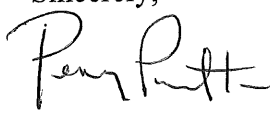
With respect to references to national security, law enforcement, and public interest purposes in the Privacy Shield Principles, I refer you to the following letters addressed to the Department of Commerce, which are publicly available at www.privacyshield.gov:

- Two letters prepared by the Office of the Director of National Intelligence (ODNI) regarding safeguards and limitations applicable to U.S. national security authorities; 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.

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

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

January 9, 2017

Federal Councillor
Johann N. Schneider-Ammann
Head of the Department of Economic Affairs, Education
and Research
Bundeshaus Ost
3003 Bern

Dear Federal Councillor:

On behalf of the International Trade Administration, I am pleased to describe the enhanced protection of personal data that the Swiss-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 in both Switzerland and the United States. It offers confidence to Swiss 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 Swiss and American businesses can continue to invest and do business across our borders. We look forward to continuing to work with the Swiss Administration and the Federal Data Protection and Information Commissioner ("the Commissioner") to ensure that the Privacy Shield functions as intended.

We have worked with the Swiss Administration to develop the Privacy Shield, modeled on the EU-U.S. Privacy Shield Framework, to allow organizations established in the United States to meet the adequacy requirements for data protection under Swiss 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 Swiss 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 Swiss 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 Swiss companies in the United States to receive personal data from Switzerland to facilitate data flows that support transatlantic trade. The U.S.-Swiss economic relationship is significant, with total goods and services trade exceeding $100 billion in 2015, supporting jobs on both sides of the Atlantic. Businesses that rely on Swiss-U.S. data flows come from all

industry sectors and include major Fortune 500 firms as well as many small and medium-sized enterprises (SMEs). With $153 billion in total investment, the U.S. is one of the largest sources of foreign investment in Switzerland and Switzerland is the 7th largest source of foreign investment in the United States with $225 billion supporting more than 470,000 jobs.

Data flows from Switzerland to the United States allow U.S. organizations to process data required to offer goods, services, and employment opportunities to Swiss individuals. The Privacy Shield supports shared privacy principles, bridging the differences in our legal approaches, while furthering trade and economic objectives of both Switzerland and the United States.

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 the Commissioner 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.

To give organizations time to review the Principles and the commitments they entail, the Department will begin accepting self-certifications 90 days after the effective date. The Principles apply immediately upon certification.

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 Switzerland;
    - 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 Commissioner, indicated its intention to cooperate with the Commissioner in the investigation and resolution of complaints brought under the Privacy Shield, notably to respond to their inquiries when Swiss data subjects have brought their complaints directly to the Commissioner;
    - 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 Switzerland for use in the context of the employment relationship, declared its commitment to cooperate and comply with the Commissioner 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 Commissioner 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: individuals in Europe, European businesses, and U.S. businesses. The inclusion of material targeted directly to individuals and European businesses will facilitate transparency in a number of ways. With regard to individuals, it will clearly explain: (1) the rights the Privacy Shield provides to Swiss individuals; (2) the recourse mechanisms available to Swiss 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 European 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 the Commissioner

To increase opportunities for cooperation with the Commissioner, the Department will establish a dedicated contact at the Department to act as a liaison with the Commissioner. In instances where the Commissioner believes that an organization is not complying with the Principles, including following a complaint from a Swiss individual, the Commissioner 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 the Commissioner seeking information related to a specific organization's self-

certification or previous participation in the program, and the contact will respond to the Commissioner's inquiries regarding the implementation of specific Privacy Shield requirements. Second, the Department will provide the Commissioner with material regarding the Privacy Shield for inclusion on its own website to increase transparency for Swiss individuals and Swiss 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 the Commissioner 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 Commissioner. To facilitate the submission of such complaints, the Department will create a standard form for the Commissioner to submit to the Department's dedicated contact. The dedicated contact will track all referrals from the Commissioner 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.

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 Swiss Administration and the Commissioner, 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 the Commissioner, the results of *ex officio* compliance reviews, and may also include discussion of relevant changes of law.

Implement the Arbitral Model

At the first annual review, the Department will work with the Swiss Administration to put in place the binding arbitration option in Annex I.

Update of Laws

The Department will make reasonable efforts to inform the Swiss Administration and the Commissioner of material developments in the law in the United States so far as they are relevant to the Privacy Shield in the field of data privacy protection and the limitations and safeguards applicable to access to personal data by U.S. authorities and its subsequent use.

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 two letters addressed to Justin Antonipillai and Ted Dean of the Department of Commerce, and we refer you to these letters which are publicly available. These letters extensively discuss, among other things, the policies, safeguards, and limitations that apply to signals intelligence activities conducted by the U.S. In addition, these letters describe the transparency provided by the Intelligence Community about these matters. As the Swiss authorities are assessing the Privacy Shield Framework, the information in these letters 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 Swiss authorities will determine that the Swiss-U.S. Privacy Shield Framework provides adequate protection for the purposes of Swiss law and data transfers from Switzerland will continue to organizations that participate in the Privacy Shield.

Sincerely,

Ken Hyatt, Acting

Swiss-U.S. Privacy Shield Principles

SWISS-U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES
ISSUED BY THE U.S. DEPARTMENT OF COMMERCE

I. OVERVIEW

1. While the United States and Switzerland share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by Switzerland. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation. Given those differences and to provide organizations in the United States with a reliable mechanism for personal data transfers to the United States from Switzerland while ensuring that Swiss data subjects continue to benefit from effective safeguards and protection as required by Swiss legislation with respect to the processing of their personal data when they have been transferred to other countries, the Department of Commerce is issuing these Privacy Shield Principles, including the Supplemental Principles (collectively "the Principles") under its statutory authority to foster, promote, and develop international commerce (15 U.S.C. § 1512). As the Swiss and EU law on data protection may be considered equivalent, the Swiss-U.S. Privacy Shield Principles and Supplemental Principles are modeled on the Principles and Supplemental Principles developed for the EU-U.S. Privacy Shield Framework. They are intended for use solely by organizations in the United States receiving personal data from Switzerland for the purpose of qualifying for the Privacy Shield and thus benefitting from Switzerland's recognition of adequacy. The Principles do not affect the application of national provisions implementing the Federal Act on Data Protection ("FADP") that apply to the processing of personal data in Switzerland. Nor do the Principles limit privacy obligations that otherwise apply under U.S. law.

2. In order to rely on the Privacy Shield to effectuate transfers of personal data from Switzerland, an organization must self-certify its adherence to the Principles to the Department of Commerce (or its designee) ("the Department"). While decisions by organizations to thus enter the Privacy Shield are entirely voluntary, effective compliance is compulsory: organizations that self-certify to the Department and publicly declare their commitment to adhere to the Principles must comply fully with the Principles. In order to enter the Privacy Shield, an organization must (a) be subject to the investigatory and enforcement powers of the Federal Trade Commission (the "FTC"), the Department of Transportation or another statutory body that will effectively ensure compliance with the Principles *(other U.S. statutory bodies recognized by Switzerland may be included as an annex in the future)*; (b) publicly declare its commitment to comply with the Principles; (c) publicly disclose its privacy policies in line with these Principles; and (d) fully implement them. An organization's failure to comply is enforceable under Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive acts in or affecting commerce (15 U.S.C. § 45(a)) or other laws or regulations prohibiting such acts.

3. The Department of Commerce will 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"). Privacy Shield benefits are assured from the date that the Department places the organization on the Privacy Shield List. The Department will remove an organization from the Privacy Shield List if it voluntarily withdraws from the Privacy Shield or if it fails to complete its annual re-certification to the Department. An organization's removal from the Privacy Shield List means it may no longer benefit from Switzerland's recognition of adequacy to receive personal information from Switzerland. The organization must continue to apply the Principles to the personal information it received while it participated in the Privacy Shield, and affirm to the Department on an annual basis its commitment to do so, for as long as it retains such information; otherwise, the organization must return or delete the information or provide "adequate" protection for the information by another authorized means. The Department will also remove from the Privacy Shield List those organizations that have persistently failed to comply with the Principles; these organizations do not qualify for Privacy Shield benefits and must return or delete the personal information they received under the Privacy Shield.

4. 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. The Department will provide a clear warning that these organizations are not participants in the Privacy Shield; that removal from the Privacy Shield List means that such organizations cannot claim to be Privacy Shield compliant and must avoid any statements or misleading practices implying that they participate in the Privacy Shield; and that such organizations are no longer entitled to benefit from Switzerland's recognition of adequacy that would enable those organizations to receive personal information from Switzerland. An organization that continues to claim participation in the Privacy Shield or makes other Privacy Shield-related misrepresentations after it has been removed from the Privacy Shield List may be subject to enforcement action by the FTC, the Department of Transportation, or other enforcement authorities.

5. Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that creates conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or (c) if the effect of Swiss data protection measures is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts. Consistent with the goal of enhancing privacy protection, organizations should strive to implement these Principles fully and transparently,

including indicating in their privacy policies where exceptions to the Principles permitted by (b) above will apply on a regular basis. For the same reason, where the option is allowable under the Principles and/or U.S. law, organizations are expected to opt for the higher protection where possible.

6. Organizations are obligated to apply the Principles to all personal data transferred in reliance on the Privacy Shield after they enter the Privacy Shield. An organization that chooses to extend Privacy Shield benefits to human resources personal information transferred from Switzerland for use in the context of an employment relationship must indicate this when it self-certifies to the Department and conform to the requirements set forth in the Supplemental Principle on Self-Certification.

7. U.S. law will apply to questions of interpretation and compliance with the Principles and relevant privacy policies by Privacy Shield organizations, except where such organizations have committed to cooperate with the Federal Data Protection and Information Commissioner (the "Commissioner"). Unless otherwise stated, all provisions of the Principles apply where they are relevant.

8. Definitions:

   a. "Personal data" and "personal information" are data about an identified or identifiable individual that are within the scope of the FADP, received by an organization in the United States from Switzerland, and recorded in any form.

   b. "Processing" of personal data means any operation or set of operations which is performed upon personal data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure or dissemination, and erasure or destruction.

   c. "Controller" means a person or organization which, alone or jointly with others, determines the purposes and means of the processing of personal data.

9. The effective date of the Principles is the date of final approval of Switzerland's recognition of adequacy.

II. PRINCIPLES

1. NOTICE

a. An organization must inform individuals about:

i. its participation in the Privacy Shield and provide a link to, or the web address for, the Privacy Shield List,

ii. the types of personal data collected and, where applicable, the entities or subsidiaries of the organization also adhering to the Principles,

iii. its commitment to subject to the Principles all personal data received from Switzerland in reliance on the Privacy Shield,

iv. the purposes for which it collects and uses personal information about them,

v. how to contact the organization with any inquiries or complaints, including any relevant establishment in Switzerland that can respond to such inquiries or complaints,

vi. the type or identity of third parties to which it discloses personal information, and the purposes for which it does so,

vii. the right of individuals to access their personal data,

viii. the choices and means the organization offers individuals for limiting the use and disclosure of their personal data,

ix. the independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual, and whether it is: (1) the Commissioner, (2) an alternative dispute resolution provider based in Switzerland, or (3) an alternative dispute resolution provider based in the United States,

x. being subject to the investigatory and enforcement powers of the FTC, the Department of Transportation or any other U.S. authorized statutory body,

xi. the possibility, under certain conditions, for the individual to invoke binding arbitration,

xii. the requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements, and

xiii. its liability in cases of onward transfers to third parties.

b. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.

2. CHOICE

a. An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals. Individuals must be provided with clear, conspicuous, and readily available mechanisms to exercise choice.

b. By derogation to the previous paragraph, it is not necessary to provide choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. However, an organization shall always enter into a contract with the agent.

c. For sensitive information (*i.e.*, personal information specifying medical or health conditions, personal sexuality, racial or ethnic origin, political opinions, religious, ideological or trade union-related views or activities, or information on social security measures or administrative or criminal proceedings and sanctions, which are treated outside pending proceedings), organizations must obtain affirmative express consent (opt in) from individuals if such information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorized by the individuals through the exercise of opt-in choice. In addition, an organization should treat as sensitive any personal information received from a third party where the third party identifies and treats it as sensitive.

3. ACCOUNTABILITY FOR ONWARD TRANSFER

a. To transfer personal information to a third party acting as a controller, organizations must comply with the Notice and Choice Principles. Organizations must also enter into a contract with the third-party controller 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 and will notify the organization if it makes a determination that it can no longer meet this obligation. The contract shall provide that when such a determination is made the third party controller ceases processing or takes other reasonable and appropriate steps to remediate.

b. To transfer personal data to a third party acting as an agent, organizations must: (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) 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; (iv) require the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles; (v) upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.

4. SECURITY

a. Organizations creating, maintaining, using or disseminating personal information must take reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.

5. DATA INTEGRITY AND PURPOSE LIMITATION

a. Consistent with the Principles, personal information must be limited to the information that is relevant for the purposes of processing.[1] An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or

[1] Depending on the circumstances, examples of compatible processing purposes may include those that reasonably serve customer relations, compliance and legal considerations, auditing, security and fraud prevention, preserving or defending the organization's legal rights, or other purposes consistent with the expectations of a reasonable person given the context of the collection.

subsequently authorized by the individual. To the extent necessary for those purposes, an organization must take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and current. An organization must adhere to the Principles for as long as it retains such information.

b. Information may be retained in a form identifying or making identifiable[2] the individual only for as long as it serves a purpose of processing within the meaning of 5a. This obligation does not prevent organizations from processing personal information for longer periods for the time and to the extent such processing reasonably serves the purposes of archiving in the public interest, journalism, literature and art, scientific or historical research, and statistical analysis. In these cases, such processing shall be subject to the other Principles and provisions of the Framework. Organizations should take reasonable and appropriate measures in complying with this provision.

6. ACCESS

a. Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

7. RECOURSE, ENFORCEMENT AND LIABILITY

a. Effective privacy protection must include robust mechanisms for assuring compliance with the Principles, recourse for individuals who are affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum such mechanisms must include:

i. readily available independent recourse mechanisms by which each individual's complaints and disputes are investigated and expeditiously resolved at no cost to the individual and by reference to the Principles, and damages awarded where the applicable law or private-sector initiatives so provide;

[2] In this context, if, given the means of identification reasonably likely to be used (considering, among other things, the costs of and the amount of time required for identification and the available technology at the time of the processing) and the form in which the data is retained, an individual could reasonably be identified by the organization, or a third party if it would have access to the data, then the individual is "identifiable."

ii. follow-up procedures for verifying that the attestations and assertions organizations make about their privacy practices are true and that privacy practices have been implemented as presented and, in particular, with regard to cases of non-compliance; and

iii. obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

b. Organizations and their selected independent recourse mechanisms will respond promptly to inquiries and requests by the Department for information relating to the Privacy Shield. All organizations must respond expeditiously to complaints regarding compliance with the Principles referred by the Commissioner through the Department. Organizations that have chosen to cooperate with the Commissioner, including organizations that process human resources data, must respond directly to such authorities with regard to the investigation and resolution of complaints.

c. Organizations are obligated to arbitrate claims and follow the terms as set forth in Annex I, provided that an individual has invoked binding arbitration by delivering notice to the organization at issue and following the procedures and subject to conditions set forth in Annex I.

d. In the context of an onward transfer, a Privacy Shield organization has responsibility 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. 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.

e. When an organization becomes subject to an FTC or court order based on non-compliance, the organization shall make public any relevant Privacy Shield-related sections of any compliance or assessment report submitted to the FTC, to the extent consistent with confidentiality requirements. The Department has established a dedicated point of contact for the Commissioner for any problems of compliance by Privacy Shield organizations. The FTC will give priority consideration to referrals of non-compliance with the Principles from the Department and the Commissioner, and will exchange information regarding referrals with the referring state authority on a timely basis, subject to existing confidentiality restrictions.

III. SUPPLEMENTAL PRINCIPLES

1. Sensitive Data

a. An organization is not required to obtain affirmative express consent (opt in) with respect to sensitive data where the processing is:

i. in the vital interests of the data subject or another person;

ii. necessary for the establishment of legal claims or defenses;

iii. required to provide medical care or diagnosis;

iv. carried out in the course of legitimate activities by a foundation, association or any other non-profit body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to the persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects;

v. necessary to carry out the organization's obligations in the field of employment law; or

vi. related to data that are manifestly made public by the individual.

2. Journalistic Exceptions

a. Given U.S. constitutional protections for freedom of the press and the Swiss exemption for journalistic material, where the rights of a free press embodied in the First Amendment of the U.S. Constitution intersect with privacy protection interests, the First Amendment must govern the balancing of these interests with regard to the activities of U.S. persons or organizations.

b. Personal information that is gathered for publication, broadcast, or other forms of public communication of journalistic material, whether used or not, as well as information found in previously published material disseminated from media archives, is not subject to the requirements of the Privacy Shield Principles.

3. Secondary Liability

a. Internet Service Providers ("ISPs"), telecommunications carriers, and other organizations are not liable under the Privacy Shield Principles when on behalf of another organization they merely transmit, route, switch, or cache information. As is the case with the FADP itself, the Privacy Shield does not create secondary liability. To the extent that an organization is acting as a mere conduit for data transmitted by third parties and does not

determine the purposes and means of processing those personal data, it would not be liable.

4. Performing Due Diligence and Conducting Audits

a. The activities of auditors and investment bankers may involve processing personal data without the consent or knowledge of the individual. This is permitted by the Notice, Choice, and Access Principles under the circumstances described below.

b. Public stock corporations and closely held companies, including Privacy Shield organizations, are regularly subject to audits. Such audits, particularly those looking into potential wrongdoing, may be jeopardized if disclosed prematurely. Similarly, a Privacy Shield organization involved in a potential merger or takeover will need to perform, or be the subject of, a "due diligence" review. This will often entail the collection and processing of personal data, such as information on senior executives and other key personnel. Premature disclosure could impede the transaction or even violate applicable securities regulation. Investment bankers and attorneys engaged in due diligence, or auditors conducting an audit, may process information without knowledge of the individual only to the extent and for the period necessary to meet statutory or public interest requirements and in other circumstances in which the application of these Principles would prejudice the legitimate interests of the organization. These legitimate interests include the monitoring of organizations' compliance with their legal obligations and legitimate accounting activities, and the need for confidentiality connected with possible acquisitions, mergers, joint ventures, or other similar transactions carried out by investment bankers or auditors.

5. The Role of the Federal Data Protection and Information Commissioner

a. Organizations will implement their commitment to cooperate with the Federal Data Protection and Information Commissioner (the "Commissioner") as described below. Under the Privacy Shield, U.S. organizations receiving personal data from Switzerland must commit to employ effective mechanisms for assuring compliance with the Privacy Shield Principles. More specifically as set out in the Recourse, Enforcement and Liability Principle, participating organizations must provide: (a)(i) recourse for individuals to whom the data relate; (a)(ii) follow up procedures for verifying that the attestations and assertions they have made about their privacy practices are true; and (a)(iii) obligations to remedy problems arising out of failure to comply with the Principles and consequences for such organizations. An organization may satisfy points (a)(i) and (a)(iii) of the Recourse, Enforcement and Liability Principle if it adheres to the requirements set forth here for cooperating with the Commissioner.

b. An organization commits to cooperate with the Commissioner by declaring in its Privacy Shield self-certification submission to the Department of Commerce (*see* Supplemental Principle on Self-Certification) that the organization:

i. elects to satisfy the requirement in points (a)(i) and (a)(iii) of the Privacy Shield Recourse, Enforcement and Liability Principle by committing to cooperate with the Commissioner;

ii. will cooperate with the Commissioner in the investigation and resolution of complaints brought under the Privacy Shield; and

iii. will comply with any advice given by the Commissioner where the Commissioner takes the view that the organization needs to take specific action to comply with the Privacy Shield Principles, including remedial or compensatory measures for the benefit of individuals affected by any non-compliance with the Principles, and will provide the Commissioner with written confirmation that such action has been taken.

c. Cooperation with the Commissioner

i. The cooperation with the Commissioner will be provided in the form of information and advice in the following way:

1. The advice of the Commissioner will be delivered directly.

2. The Commissioner will provide advice to the U.S. organizations concerned on unresolved complaints from individuals about the handling of personal information that has been transferred from Switzerland under the Privacy Shield. This advice will be designed to ensure that the Privacy Shield Principles are being correctly applied and will include any remedies for the individual(s) concerned that the Commissioner considers appropriate.

3. The Commissioner will provide such advice in response to referrals from the organizations concerned and/or to complaints received directly from individuals against organizations which have committed to cooperate with the Commissioner for Privacy Shield purposes, while encouraging and if necessary helping such individuals in the first instance to use the in-house complaint handling arrangements that the organization may offer.

4. Advice will be issued only after both sides in a dispute have had a reasonable opportunity to comment and to provide any evidence they wish. The Commissioner will seek to deliver advice as quickly as this requirement for due process allows. As a general rule, the Commissioner will aim to provide

advice within 60 days after receiving a complaint or referral and more quickly where possible.

5. The Commissioner will make public the results of its consideration of complaints submitted to it, if it sees fit.

6. The delivery of advice through the Commissioner will not give rise to any liability for the Commissioner.

ii. As noted above, organizations choosing this option for dispute resolution must undertake to comply with the advice of the Commissioner. If an organization fails to comply within 25 days of the delivery of the advice and has offered no satisfactory explanation for the delay, the Commissioner will give notice of its intention either to refer the matter to the Federal Trade Commission, the Department of Transportation, or other U.S. federal or state body with statutory powers to take enforcement action in cases of deception or misrepresentation, or to conclude that the agreement to cooperate has been seriously breached and must therefore be considered null and void. In the latter case, the Commissioner will inform the Department of Commerce so that the Privacy Shield List can be duly amended. Any failure to fulfill the undertaking to cooperate with the Commissioner, as well as failures to comply with the Privacy Shield Principles, will be actionable as a deceptive practice under Section 5 of the FTC Act or other similar statute.

d. An organization that wishes its Privacy Shield benefits to cover human resources data transferred from Switzerland in the context of the employment relationship must commit to cooperate with the Commissioner with regard to such data (*see* Supplemental Principle on Human Resources Data).

6. Self-Certification

a. Privacy Shield benefits are assured from the date on which the Department has placed the organization's self-certification submission on the Privacy Shield List after having determined that the submission is complete.

b. To self-certify for the Privacy Shield, an organization must provide to the Department a self-certification submission, signed by a corporate officer on behalf of the organization that is joining the Privacy Shield, that contains at least the following information:

i. name of organization, mailing address, e-mail address, telephone, and fax numbers;

ii. description of the activities of the organization with respect to personal information received from Switzerland; and

iii. description of the organization's privacy policy for such personal information, including:

1. if the organization has a public website, the relevant web address where the privacy policy is available, or if the organization does not have a public website, where the privacy policy is available for viewing by the public;

2. its effective date of implementation;

3. a contact office for the handling of complaints, access requests, and any other issues arising under the Privacy Shield;

4. 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);

5. name of any privacy program in which the organization is a member;

6. method of verification (*e.g.*, in-house, third party) (*see* Supplemental Principle on Verification); and

7. the independent recourse mechanism that is available to investigate unresolved complaints.

c. Where the organization wishes its Privacy Shield benefits to cover human resources information transferred from Switzerland for use in the context of the employment relationship, it may do so where a statutory body listed in the Principles or a future annex to the Principles has jurisdiction to hear claims against the organization arising out of the processing of human resources information. In addition, the organization must indicate this in its self-certification submission and declare its commitment to cooperate with the Commissioner in conformity with the Supplemental Principles on Human Resources Data and the Role of the Federal Data Protection and Information Commissioner as applicable and that it will comply with the advice given by the Commissioner. The organization must also provide the Department with a copy of its human resources privacy policy and provide information where the privacy policy is available for viewing by its affected employees.

d. The Department will maintain the Privacy Shield List of organizations that file completed self-certification submissions, thereby assuring the availability of Privacy Shield benefits, and will update such list on the basis of annual self-recertification submissions and notifications received pursuant to the Supplemental Principle on Dispute Resolution and Enforcement. Such self-certification submissions must be provided not less than annually; otherwise the organization will be removed from the Privacy Shield List and Privacy Shield benefits will no longer be assured. Both the Privacy Shield List and the self-certification submissions by the

organizations will be made publicly available. All organizations that are placed on the Privacy Shield List by the Department must also state in their relevant published privacy policy statements that they adhere to the Privacy Shield Principles. If available online, an organization's privacy policy must include a hyperlink to the Department's Privacy Shield website and a hyperlink to the website or complaint submission form of the independent recourse mechanism that is available to investigate unresolved complaints.

e. The Privacy Principles apply immediately upon certification.

f. An organization must subject to the Privacy Shield Principles all personal data received from Switzerland in reliance upon the Privacy Shield. The undertaking to adhere to the Privacy Shield Principles is not time-limited in respect of personal data received during the period in which the organization enjoys the benefits of the Privacy Shield. Its 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 Privacy Shield for any reason. An organization that withdraws from the Privacy Shield but wants to retain such data must affirm to the Department on an annual basis its commitment to continue to apply the Principles or provide "adequate" protection for the information by another authorized means (for example, using a contract that fully reflects the requirements of the relevant standard contractual clauses adopted by the Commissioner); otherwise, the organization must return or delete the information. An organization that withdraws from the Privacy Shield must remove from any relevant 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.

g. An organization that will cease to exist as a separate legal entity as a result of a merger or a takeover must notify the Department of this in advance. The notification should also indicate whether the acquiring entity or the entity resulting from the merger will (i) continue to be bound by the Privacy Shield Principles by the operation of law governing the takeover or merger or (ii) elect to self-certify its adherence to the Privacy Shield Principles or put in place other safeguards, such as a written agreement that will ensure adherence to the Privacy Shield Principles. Where neither (i) nor (ii) applies, any personal data that has been acquired under the Privacy Shield must be promptly deleted.

h. When an organization leaves the Privacy Shield for any reason, it must remove all statements implying that the organization continues to participate in the Privacy Shield or is entitled to the benefits of the Privacy Shield. The Swiss-U.S. Privacy Shield certification mark, if used, must also be removed. Any misrepresentation to the general public concerning an organization's adherence to the Privacy Shield Principles may be actionable by the FTC or other relevant government body. Misrepresentations to the

Department may be actionable under the False Statements Act (18 U.S.C. § 1001).

7. Verification

a. Organizations must provide follow up procedures for verifying that the attestations and assertions they make about their Privacy Shield privacy practices are true and those privacy practices have been implemented as represented and in accordance with the Privacy Shield Principles.

b. To meet the verification requirements of the Recourse, Enforcement and Liability Principle, an organization must verify such attestations and assertions either through self-assessment or outside compliance reviews.

c. Under the self-assessment approach, such verification must indicate that an organization's published privacy policy regarding personal information received from Switzerland is accurate, comprehensive, prominently displayed, completely implemented and accessible. It must also indicate that its privacy policy conforms to the Privacy Shield Principles; that individuals are informed of any in-house arrangements for handling complaints and of the independent mechanisms through which they may pursue complaints; that it has in place procedures for training employees in its implementation, and disciplining them for failure to follow it; and that it has in place internal procedures for periodically conducting objective reviews of compliance with the above. A statement verifying the self-assessment must be signed by a corporate officer or other authorized representative of the organization at least once a year and made available upon request by individuals or in the context of an investigation or a complaint about non-compliance.

d. Where the organization has chosen outside compliance review, such a review must demonstrate that its privacy policy regarding personal information received from Switzerland conforms to the Privacy Shield Principles, that it is being complied with, and that individuals are informed of the mechanisms through which they may pursue complaints. The methods of review may include, without limitation, auditing, random reviews, use of "decoys", or use of technology tools as appropriate. A statement verifying that an outside compliance review has been successfully completed must be signed either by the reviewer or by the corporate officer or other authorized representative of the organization at least once a year and made available upon request by individuals or in the context of an investigation or a complaint about compliance.

e. Organizations must retain their records on the implementation of their Privacy Shield privacy practices and make them available upon request in the context of an investigation or a complaint about non-compliance to the independent body responsible for investigating complaints or to the agency with unfair and deceptive practices jurisdiction. Organizations must also

respond promptly to inquiries and other requests for information from the Department relating to the organization's adherence to the Principles.

8. Access

a. The Access Principle in Practice

i. Under the Privacy Shield Principles, the right of access is fundamental to privacy protection. In particular, it allows individuals to verify the accuracy of information held about them. The Access Principle means that individuals have the right to:

1. obtain from an organization confirmation of whether or not the organization is processing personal data relating to them;[3]

2. have communicated to them such data so that they could verify its accuracy and the lawfulness of the processing; and

3. have the data corrected, amended or deleted where it is inaccurate or processed in violation of the Principles.

ii. Individuals do not have to justify requests for access to their personal data. In responding to individuals' access requests, organizations should first be guided by the concern(s) that led to the requests in the first place. For example, if an access request is vague or broad in scope, an organization may engage the individual in a dialogue so as to better understand the motivation for the request and to locate responsive information. The organization might inquire about which part(s) of the organization the individual interacted with or about the nature of the information or its use that is the subject of the access request.

iii. Consistent with the fundamental nature of access, organizations should always make good faith efforts to provide access. For example, where certain information needs to be protected and can be readily separated from other personal information subject to an access request, the organization should redact the protected information and make available the other information. If an organization determines that access should be restricted in any particular instance, it should provide the individual requesting access with an explanation of why it has made that determination and a contact point for any further inquiries.

[3] The organization should answer requests from an individual concerning the purposes of the processing, the categories of personal data concerned, and the recipients or categories of recipients to whom the personal data is disclosed.

b. Burden or Expense of Providing Access

i. The right of access to personal data may be restricted in exceptional circumstances where the legitimate rights of persons other than the individual would be violated or where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question. Expense and burden are important factors and should be taken into account but they are not controlling factors in determining whether providing access is reasonable.

ii. For example, if the personal information is used for decisions that will significantly affect the individual (*e.g.*, the denial or grant of important benefits, such as insurance, a mortgage, or a job), then consistent with the other provisions of these Supplemental Principles, the organization would have to disclose that information even if it is relatively difficult or expensive to provide. If the personal information requested is not sensitive or not used for decisions that will significantly affect the individual, but is readily available and inexpensive to provide, an organization would have to provide access to such information.

c. Confidential Commercial Information

i. Confidential commercial information is information that an organization has taken steps to protect from disclosure, where disclosure would help a competitor in the market. Organizations may deny or limit access to the extent that granting full access would reveal its own confidential commercial information, such as marketing inferences or classifications generated by the organization, or the confidential commercial information of another that is subject to a contractual obligation of confidentiality.

ii. Where confidential commercial information can be readily separated from other personal information subject to an access request, the organization should redact the confidential commercial information and make available the non-confidential information.

d. Organization of Data Bases

i. Access can be provided in the form of disclosure of the relevant personal information by an organization to the individual and does not require access by the individual to an organization's data base.

ii. Access needs to be provided only to the extent that an organization stores the personal information. The Access Principle does not itself create any obligation to retain, maintain, reorganize, or restructure personal information files.

e. When Access May be Restricted

i. As organizations must always make good faith efforts to provide individuals with access to their personal data, the circumstances in which organizations may restrict such access are limited, and any reasons for restricting access must be specific. As under the FADP, an organization can restrict access to information to the extent that disclosure is likely to interfere with the safeguarding of important countervailing public interests, such as national security; defense; or public security. In addition, where personal information is processed solely for research or statistical purposes, access may be denied. Other reasons for denying or limiting access are:

1. interference with the execution or enforcement of the law or with private causes of action, including the prevention, investigation or detection of offenses or the right to a fair trial;

2. disclosure where the legitimate rights or important interests of others would be violated;

3. breaching a legal or other professional privilege or obligation;

4. prejudicing employee security investigations or grievance proceedings or in connection with employee succession planning and corporate re-organizations; or

5. prejudicing the confidentiality necessary in monitoring, inspection or regulatory functions connected with sound management, or in future or ongoing negotiations involving the organization.

ii. An organization which claims an exception has the burden of demonstrating its necessity, and the reasons for restricting access and a contact point for further inquiries should be given to individuals.

f. Right to Obtain Confirmation and Charging a Fee to Cover the Costs for Providing Access

i. An individual has the right to obtain confirmation of whether or not this organization has personal data relating to him or her. An individual also has the right to have communicated to him or her personal data relating to him or her. An organization may charge a fee that is not excessive.

ii. Charging a fee may be justified, for example, where requests for access are manifestly excessive, in particular because of their repetitive character.

iii. Access may not be refused on cost grounds if the individual offers to pay the costs.

g. Repetitious or Vexatious Requests for Access

i. An organization may set reasonable limits on the number of times within a given period that access requests from a particular individual will be met. In setting such limitations, an organization should consider such factors as the frequency with which information is updated, the purpose for which the data are used, and the nature of the information.

h. Fraudulent Requests for Access

i. An organization is not required to provide access unless it is supplied with sufficient information to allow it to confirm the identity of the person making the request.

i. Timeframe for Responses

i. Organizations should respond to access requests within a reasonable time period, in a reasonable manner, and in a form that is readily intelligible to the individual. An organization that provides information to data subjects at regular intervals may satisfy an individual access request with its regular disclosure if it would not constitute an excessive delay.

9. Human Resources Data

a. Coverage by the Privacy Shield

i. Where an organization in Switzerland transfers personal information about its employees (past or present) collected in the context of the employment relationship, to a parent, affiliate, or unaffiliated service provider in the United States participating in the Privacy Shield, the transfer enjoys the benefits of the Privacy Shield. In such cases, the collection of the information and its processing prior to transfer will have been subject to the national laws of Switzerland, and any conditions for or restrictions on its transfer according to those laws will have to be respected.

ii. The Privacy Shield Principles are relevant only when individually identified or identifiable records are transferred or accessed. Statistical reporting relying on aggregate employment data and containing no personal data or the use of anonymized data does not raise privacy concerns.

b. Application of the Notice and Choice Principles

i. A U.S. organization that has received employee information from Switzerland under the Privacy Shield may disclose it to third parties

or use it for different purposes only in accordance with the Notice and Choice Principles. For example, where an organization intends to use personal information collected through the employment relationship for non-employment-related purposes, such as marketing communications, the U.S. organization must provide the affected individuals with the requisite choice before doing so, unless they have already authorized the use of the information for such purposes. Such use must not be incompatible with the purposes for which the personal information has been collected or subsequently authorized by the individual. Moreover, such choices must not be used to restrict employment opportunities or take any punitive action against such employees.

ii. In addition, employers should make reasonable efforts to accommodate employee privacy preferences. This could include, for example, restricting access to the personal data, anonymizing certain data, or assigning codes or pseudonyms when the actual names are not required for the management purpose at hand.

iii. To the extent and for the period necessary to avoid prejudicing the ability of the organization in making promotions, appointments, or other similar employment decisions, an organization does not need to offer notice and choice.

c. Application of the Access Principle

i. The Supplemental Principle on Access provides guidance on reasons which may justify denying or limiting access on request in the human resources context. Of course, employers in Switzerland must comply with local regulations and ensure that Swiss employees have access to such information as is required by Swiss law, regardless of the location of data processing and storage. The Privacy Shield requires that an organization processing such data in the United States will cooperate in providing such access either directly or through the Swiss employer.

d. Enforcement

i. In so far as personal information is used only in the context of the employment relationship, primary responsibility for the data vis-à-vis the employee remains with the organization in Switzerland. It follows that, where Swiss employees make complaints about violations of their data protection rights and are not satisfied with the results of internal review, complaint, and appeal procedures (or any applicable grievance procedures under a contract with a trade union), they should be directed to the Commissioner or labor authority in the jurisdiction where the employees work. This includes cases where the alleged mishandling of their personal information is the responsibility of the U.S. organization that has

received the information from the employer and thus involves an alleged breach of the Privacy Shield Principles. This will be the most efficient way to address the often overlapping rights and obligations imposed by local labor law and labor agreements as well as data protection law.

ii. A U.S. organization participating in the Privacy Shield that uses Swiss human resources data transferred from Switzerland in the context of the employment relationship and that wishes such transfers to be covered by the Privacy Shield must therefore commit to cooperate in investigations by and to comply with the advice of the Commissioner in such cases.

e. Application of the Accountability for Onward Transfer Principle

i. For occasional employment-related operational needs of the Privacy Shield organization with respect to personal data transferred under the Privacy Shield, such as the booking of a flight, hotel room, or insurance coverage, transfers of personal data of a small number of employees can take place to controllers without application of the Access Principle or entering into a contract with the third-party controller, as otherwise required under the Accountability for Onward Transfer Principle, provided that the Privacy Shield organization has complied with the Notice and Choice Principles.

10. Obligatory Contracts for Onward Transfers

a. Data Processing Contracts

i. When personal data is transferred from Switzerland to the United States only for processing purposes, a contract will be required, regardless of participation by the processor in the Privacy Shield.

ii. Data controllers in Switzerland 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 Switzerland, and whether or not the processor participates in the Privacy Shield. The purpose of the contract is to make sure that the processor:

1. acts only on instructions from the controller;

2. provides appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and understands whether onward transfer is allowed; and

3. taking into account the nature of the processing, assists the controller in responding to individuals exercising their rights under the Principles.

iii. Because adequate protection is provided by Privacy Shield participants, contracts with Privacy Shield participants for mere processing do not require prior authorization (or such authorization will be granted automatically by the Commissioner), as would be required for contracts with recipients not participating in the Privacy Shield or otherwise not providing adequate protection.

b. Transfers within a Controlled Group of Corporations or Entities

i. When personal information is transferred between two controllers within a controlled group of corporations or entities, a contract is not always required under the Accountability for Onward Transfer Principle. Data controllers within a controlled group of corporations or entities may base such transfers on other instruments, such as Binding Corporate Rules or other intra-group instruments (*e.g.*, compliance and control programs), ensuring the continuity of protection of personal information under the Principles. In case of such transfers, the Privacy Shield organization remains responsible for compliance with the Principles.

c. Transfers between Controllers

i. For transfers between controllers, the recipient controller need not be a Privacy Shield organization or have an independent recourse mechanism. The Privacy Shield organization must enter into a contract with the recipient third-party controller that provides for the same level of protection as is available under the Privacy Shield, not including the requirement that the third-party controller be a Privacy Shield organization or have an independent recourse mechanism, provided it makes available an equivalent mechanism.

11. Dispute Resolution and Enforcement

a. The Recourse, Enforcement and Liability Principle sets out the requirements for Privacy Shield enforcement. How to meet the requirements of point (a)(ii) of the Principle is set out in the Supplemental Principle on Verification. This Supplemental Principle addresses points (a)(i) and (a)(iii), both of which require independent recourse mechanisms. These mechanisms may take different forms, but they must meet the Recourse, Enforcement and Liability Principle's requirements. Organizations satisfy the requirements through the following: (i) compliance with private sector developed privacy programs that incorporate the Privacy Shield Principles into their rules and that include effective enforcement mechanisms of the type described in the Recourse, Enforcement and Liability Principle; (ii) compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution; or (iii) commitment to cooperate with the Commissioner or its authorized representative.

b. This list is intended to be illustrative and not limiting. The private sector may design additional mechanisms to provide enforcement, so long as they meet the requirements of the Recourse, Enforcement and Liability Principle and the Supplemental Principles. Please note that the Recourse, Enforcement and Liability Principle's requirements are additional to the requirement that self-regulatory efforts must be enforceable under Section 5 of the Federal Trade Commission Act, which prohibits unfair and deceptive acts, or another law or regulation prohibiting such acts.

c. In order to help ensure compliance with their Privacy Shield commitments and to support the administration of the program, organizations, as well as their independent recourse mechanisms, must provide information relating to the Privacy Shield when requested by the Department. In addition, organizations must respond expeditiously to complaints regarding their compliance with the Principles referred through the Department by the Commissioner. The response should address whether the complaint has merit and, if so, how the organization will rectify the problem. The Department will protect the confidentiality of information it receives in accordance with U.S. law.

d. <u>Recourse Mechanisms</u>

i. Consumers should be encouraged to raise any complaints they may have with the relevant organization before proceeding to independent recourse mechanisms. Organizations must respond to a consumer within 45 days of receiving a complaint. Whether a recourse mechanism is independent is a factual question that can be demonstrated notably by impartiality, transparent composition and financing, and a proven track record. As required by the Recourse, Enforcement and Liability Principle, the recourse available to individuals must be readily available and free of charge to individuals. Dispute resolution bodies should look into each complaint received from individuals unless they are obviously unfounded or frivolous. This does not preclude the establishment of eligibility requirements by the organization operating the recourse mechanism, but such requirements should be transparent and justified (for example, to exclude complaints that fall outside the scope of the program or are for consideration in another forum), and should not have the effect of undermining the commitment to look into legitimate complaints. In addition, recourse mechanisms should provide individuals with full and readily available information about how the dispute resolution procedure works when they file a complaint. Such information should include notice about the mechanism's privacy practices, in conformity with the Privacy Shield Principles. They should also cooperate in the development of tools such as standard complaint forms to facilitate the complaint resolution process.

ii. Independent recourse mechanisms must include on their public websites information regarding the Privacy Shield Principles and the services that they provide under the Privacy Shield. This information must include: (1) information on or a link to the Privacy Shield Principles' requirements for independent recourse mechanisms; (2) a link to the Department's Privacy Shield website; (3) an explanation that their dispute resolution services under the Privacy Shield are free of charge to individuals; (4) a description of how a Privacy Shield-related complaint can be filed; (5) the timeframe in which Privacy Shield-related complaints are processed; and (6) a description of the range of potential remedies.

iii. Independent recourse mechanisms must publish an annual report providing aggregate statistics regarding their dispute resolution services. The annual report must include: (1) the total number of Privacy Shield-related complaints received during the reporting year; (2) the types of complaints received; (3) dispute resolution quality measures, such as the length of time taken to process complaints; and (4) the outcomes of the complaints received, notably the number and types of remedies or sanctions imposed.

iv. As set forth in Annex I, an arbitration option is available to an individual to determine, for residual claims, whether a Privacy Shield organization has violated its obligations under the Principles as to that individual, and whether any such violation remains fully or partially unremedied. This option is available only for these purposes. This option is not available, for example, with respect to the exceptions to the Principles[4] or with respect to an allegation about the adequacy of the Privacy Shield. Under this arbitration option, the Privacy Shield Panel (consisting of one or three arbitrators, as agreed by the parties) has the authority to impose individual-specific, non-monetary equitable relief (such as access, correction, deletion, or return of the individual's data in question) necessary to remedy the violation of the Principles only with respect to the individual. Individuals and Privacy Shield organizations will be able to seek judicial review and enforcement of the arbitral decisions pursuant to U.S. law under the Federal Arbitration Act.

e. Remedies and Sanctions

i. The result of any remedies provided by the dispute resolution body should be that the effects of non-compliance are reversed or corrected by the organization, insofar as feasible, and that future processing by the organization will be in conformity with the Principles and, where appropriate, that processing of the personal data of the individual who brought the complaint will cease.

[4] Section I.5 of the Principles.

Sanctions need to be rigorous enough to ensure compliance by the organization with the Principles. A range of sanctions of varying degrees of severity will allow dispute resolution bodies to respond appropriately to varying degrees of non-compliance. Sanctions should include both publicity for findings of non-compliance and the requirement to delete data in certain circumstances.[5] Other sanctions could include suspension and removal of a seal, compensation for individuals for losses incurred as a result of non-compliance and injunctive awards. Private sector dispute resolution bodies and self-regulatory bodies must notify failures of Privacy Shield organizations to comply with their rulings to the governmental body with applicable jurisdiction or to the courts, as appropriate, and to notify the Department.

f. FTC Action

ii. The FTC has committed to reviewing on a priority basis referrals alleging non-compliance with the Principles received from: (i) privacy self-regulatory organizations and other independent dispute resolution bodies; (ii) the Commissioner; and (iii) the Department, 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 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. This includes false claims of adherence to the Privacy Shield Principles or participation in the Privacy Shield by organizations, which either are no longer on the Privacy Shield List or have never self-certified to the Department. 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. The FTC will notify the Department of any such actions it takes. The Department encourages other government bodies to notify it of the final disposition of any such referrals or other rulings determining adherence to the Privacy Shield Principles.

g. Persistent Failure to Comply

i. If an organization persistently fails to comply with the Principles, it is no longer entitled to benefit from the Privacy Shield. Organizations that have persistently failed to comply with the

[5] Dispute resolution bodies have discretion about the circumstances in which they use these sanctions. The sensitivity of the data concerned is one factor to be taken into consideration in deciding whether deletion of data should be required, as is whether an organization has collected, used, or disclosed information in blatant contravention of the Privacy Shield Principles.

Principles will be removed from the Privacy Shield List by the Department and must return or delete the personal information they received under the Privacy Shield.

ii. Persistent failure to comply arises where an organization that has self-certified to the Department refuses to comply with a final determination by any privacy self-regulatory, independent dispute resolution, or government body, or where such a body determines that an organization frequently fails to comply with the Principles to the point where its claim to comply is no longer credible. In these cases, the organization must promptly notify the Department of such facts. Failure to do so may be actionable under the False Statements Act (18 U.S.C. § 1001). An organization's withdrawal from a private-sector privacy self-regulatory program or independent dispute resolution mechanism does not relieve it of its obligation to comply with the Principles and would constitute a persistent failure to comply.

iii. The Department will remove an organization from the Privacy Shield List in response to any notification it receives of persistent failure to comply, whether it is received from the organization itself, from a privacy self-regulatory body or another independent dispute resolution body, or from a government body, but only after first providing 30 days' notice and an opportunity to respond to the organization that has failed to comply. Accordingly, the Privacy Shield List maintained by the Department will make clear which organizations are assured and which organizations are no longer assured of Privacy Shield benefits.

iv. An organization applying to participate in a self-regulatory body for the purposes of requalifying for the Privacy Shield must provide that body with full information about its prior participation in the Privacy Shield.

12. Choice – Timing of Opt Out

a. Generally, the purpose of the Choice Principle is to ensure that personal information is used and disclosed in ways that are consistent with the individual's expectations and choices. Accordingly, an individual should be able to exercise "opt out" choice of having personal information used for direct marketing at any time subject to reasonable limits established by the organization, such as giving the organization time to make the opt out effective. An organization may also require sufficient information to confirm the identity of the individual requesting the "opt out." In the United States, individuals may be able to exercise this option through the use of a central "opt out" program such as the Direct Marketing Association's Mail Preference Service. Organizations that participate in the Direct Marketing Association's Mail Preference Service should promote its availability to consumers who do not wish to receive commercial information. In any event, an individual should be given a readily available and affordable mechanism to exercise this option.

b. Similarly, an organization may use information for certain direct marketing purposes when it is impracticable to provide the individual with an opportunity to opt out before using the information, if the organization promptly gives the individual such opportunity at the same time (and upon request at any time) to decline (at no cost to the individual) to receive any further direct marketing communications and the organization complies with the individual's wishes.

13. Travel Information

a. Airline passenger reservation and other travel information, such as frequent flyer or hotel reservation information and special handling needs, such as meals to meet religious requirements or physical assistance, may be transferred to organizations located outside Switzerland in several different circumstances. Under Article 6(2) FADP, personal data may be transferred to a third country "in the absence of legislation that guarantees adequate protection within the meaning of Article 6(1)" on the condition that (i) it is necessary to provide the services requested by the consumer or to fulfill the terms of an agreement, such as a "frequent flyer" agreement; or (ii) it has been unambiguously consented to by the consumer in the specific case. U.S. organizations subscribing to the Privacy Shield provide adequate protection for personal data and may therefore receive data transfers from Switzerland without meeting these conditions or other conditions set out in Article 6 FADP. Since the Privacy Shield includes specific rules for sensitive information, such information (which may need to be collected, for example, in connection with customers' needs for physical assistance) may be included in transfers to Privacy Shield participants. In all cases, however, the organization transferring the information has to respect the law in Switzerland, which may inter alia impose special conditions for the handling of sensitive data.

14. Pharmaceutical and Medical Products

a. Application of Swiss Laws or the Privacy Shield Principles

i. Swiss law applies to the collection of the personal data and to any processing that takes place prior to the transfer to the United States. The Privacy Shield Principles apply to the data once they have been transferred to the United States. Data used for pharmaceutical research and other purposes should be anonymized when appropriate.

b. Future Scientific Research

i. Personal data developed in specific medical or pharmaceutical research studies often play a valuable role in future scientific research. Where personal data collected for one research study are transferred to a U.S. organization in the Privacy Shield, the organization may use the data for a new scientific research activity if appropriate notice and choice have been provided in the first instance. Such notice should provide information about any future specific uses of the data, such as periodic follow-up, related studies, or marketing.

ii. It is understood that not all future uses of the data can be specified, since a new research use could arise from new insights on the original data, new medical discoveries and advances, and public health and regulatory developments. Where appropriate, the notice should therefore include an explanation that personal data may be used in future medical and pharmaceutical research activities that are unanticipated. If the use is not consistent with the general research purpose(s) for which the personal data were originally collected, or to which the individual has consented subsequently, new consent must be obtained.

c. Withdrawal from a Clinical Trial

i. Participants may decide or be asked to withdraw from a clinical trial at any time. Any personal data collected previous to withdrawal may still be processed along with other data collected as part of the clinical trial, however, if this was made clear to the participant in the notice at the time he or she agreed to participate.

d. Transfers for Regulatory and Supervision Purposes

i. Pharmaceutical and medical device companies are allowed to provide personal data from clinical trials conducted in Switzerland to regulators in the United States for regulatory and supervision purposes. Similar transfers are allowed to parties other than regulators, such as company locations and other researchers, consistent with the Principles of Notice and Choice.

e. "Blinded" Studies

i. To ensure objectivity in many clinical trials, participants, and often investigators as well, cannot be given access to information about which treatment each participant may be receiving. Doing so would jeopardize the validity of the research study and results. Participants in such clinical trials (referred to as "blinded" studies) do not have to be provided access to the data on their treatment during the trial if this restriction has been explained when the participant entered the trial and the disclosure of such information would jeopardize the integrity of the research effort.

ii. Agreement to participate in the trial under these conditions is a reasonable forgoing of the right of access. Following the conclusion of the trial and analysis of the results, participants should have access to their data if they request it. They should seek it primarily from the physician or other health care provider from whom they received treatment within the clinical trial, or secondarily from the sponsoring organization.

f. Product Safety and Efficacy Monitoring

i. A pharmaceutical or medical device company does not have to apply the Privacy Shield Principles with respect to the Notice, Choice, Accountability for Onward Transfer, and Access Principles in its product safety and efficacy monitoring activities, including the reporting of adverse events and the tracking of patients/subjects using certain medicines or medical devices, to the extent that adherence to the Principles interferes with compliance with regulatory requirements. This is true both with respect to reports by, for example, health care providers to pharmaceutical and medical device companies, and with respect to reports by pharmaceutical and medical device companies to government agencies like the Food and Drug Administration.

g. Key-coded Data

i. Invariably, research data are uniquely key-coded at their origin by the principal investigator so as not to reveal the identity of individual data subjects. Pharmaceutical companies sponsoring such research do not receive the key. The unique key code is held only by the researcher, so that he or she can identify the research subject under special circumstances (*e.g.*, if follow-up medical attention is required). A transfer from Switzerland to the United States of data coded in this way would not constitute a transfer of personal data that would be subject to the Privacy Shield Principles.

15. Public Record and Publicly Available Information

a. An organization must apply the Privacy Shield Principles of Security, Data Integrity and Purpose Limitation, and Recourse, Enforcement and Liability to personal data from publicly available sources. These Principles shall apply also to personal data collected from public records, *i.e.*, those records kept by government agencies or entities at any level that are open to consultation by the public in general.

b. It is not necessary to apply the Notice, Choice, or Accountability for Onward Transfer Principles to public record information, as long as it is not combined with non-public record information, and any conditions for consultation established by the relevant jurisdiction are respected. Also, it is generally not necessary to apply the Notice, Choice, or Accountability for Onward Transfer Principles to publicly available information unless the Swiss transferor indicates that such information is subject to restrictions that require application of those Principles by the organization for the uses it intends. Organizations will have no liability for how such information is used by those obtaining such information from published materials.

c. Where an organization is found to have intentionally made personal information public in contravention of the Principles so that it or others may benefit from these exceptions, it will cease to qualify for the benefits of the Privacy Shield.

d. It is not necessary to apply the Access Principle to public record information as long as it is not combined with other personal information (apart from small amounts used to index or organize the public record information); however, any conditions for consultation established by the relevant jurisdiction are to be respected. In contrast, where public record information is combined with other non-public record information (other than as specifically noted above), an organization must provide access to all such information, assuming it is not subject to other permitted exceptions.

e. As with public record information, it is not necessary to provide access to information that is already publicly available to the public at large, as long as it is not combined with non-publicly available information. Organizations that are in the business of selling publicly available information may charge the organization's customary fee in responding to requests for access. Alternatively, individuals may seek access to their information from the organization that originally compiled the data.

16. Access Requests by Public Authorities

a. In order to provide transparency in respect of lawful requests by public authorities to access personal information, Privacy Shield organizations may voluntarily issue periodic transparency reports on the number of requests for personal information they receive by public authorities for law

enforcement or national security reasons, to the extent such disclosures are permissible under applicable law.

b. The information provided by the Privacy Shield organizations in these reports together with information that has been released by the intelligence community, along with other information, can be used to inform the annual joint review of the functioning of the Privacy Shield in accordance with the Principles.

c. Absence of notice in accordance with point (a)(xii) of the Notice Principle shall not prevent or impair an organization's ability to respond to any lawful request.

ANNEX I

This Annex I provides the terms under which Privacy Shield organizations are obligated to arbitrate claims, pursuant to the Recourse, Enforcement and Liability Principle. The binding arbitration option described below applies to certain "residual" claims as to data covered by the Swiss-U.S. Privacy Shield. The purpose of this option is to provide a prompt, independent, and fair mechanism, at the option of individuals, for resolution of claimed violations of the Principles not resolved by any of the other Privacy Shield mechanisms, if any. At the first annual review[1], the Department of Commerce will work with the Swiss Administration to put in place this binding arbitration option.

A. Scope

This arbitration option is available to an individual to determine, for residual claims, whether a Privacy Shield organization has violated its obligations under the Principles as to that individual, and whether any such violation remains fully or partially unremedied. This option is available only for these purposes. This option is not available, for example, with respect to the exceptions to the Principles[2] or with respect to an allegation about the adequacy of the Privacy Shield.

B. Available Remedies

Under this arbitration option, the Privacy Shield Panel (consisting of one or three arbitrators, as agreed by the parties) has the authority to impose individual-specific, non-monetary equitable relief (such as access, correction, deletion, or return of the individual's data in question) necessary to remedy the violation of the Principles only with respect to the individual. These are the only powers of the arbitration panel with respect to remedies. In considering remedies, the arbitration panel is required to consider other remedies that already have been imposed by other mechanisms under the Privacy Shield. No damages, costs, fees, or other remedies are available. Each party bears its own attorney's fees.

C. Pre-Arbitration Requirements

An individual who decides to invoke this arbitration option must take the following steps prior to initiating an arbitration claim: (1) raise the claimed violation directly with the organization and afford the organization an opportunity to resolve the issue within the timeframe set forth in Section III.11(d)(i) of the Principles; (2) make use of the independent recourse mechanism under the Principles, which is at no cost to the individual; and (3) raise the issue through the Federal Data Protection and Information Commissioner (the "Commissioner") to the Department of Commerce and afford the Department of Commerce an opportunity to use best efforts to resolve the issue within the timeframes set forth in the Letter from the International Trade Administration of the Department of Commerce, at no cost to the individual.

---

[1] As described in the letter from the International Trade Administration (ITA) of the Department of Commerce describing the commitments that ITA has made to ensure that the Privacy Shield operates effectively, including the joint review mechanism of the functioning of the Privacy Shield.

[2] Section I.5 of the Principles.

This arbitration option may not be invoked if the individual's same claimed violation of the Principles (1) has previously been subject to binding arbitration; (2) was the subject of a final judgment entered in a court action to which the individual was a party; or (3) was previously settled by the parties. In addition, this option may not be invoked if the Commissioner (1) has authority under Sections III.5 or III.9 of the Principles; or (2) has the authority to resolve the claimed violation directly with the organization. The Commissioner's authority to resolve the same claim against a Swiss data controller does not alone preclude invocation of this arbitration option against a different legal entity not bound by the Commissioner's authority.

D. Binding Nature of Decisions

An individual's decision to invoke this binding arbitration option is entirely voluntary. Arbitral decisions will be binding on all parties to the arbitration. Once invoked, the individual forgoes the option to seek relief for the same claimed violation in another forum, except that if non-monetary equitable relief does not fully remedy the claimed violation, the individual's invocation of arbitration will not preclude a claim for damages that is otherwise available in the courts.

E. Review and Enforcement

Individuals and Privacy Shield organizations will be able to seek judicial review and enforcement of the arbitral decisions pursuant to U.S. law under the Federal Arbitration Act.[3]

[3] Chapter 2 of the Federal Arbitration Act ("FAA") provides that "[a]n arbitration agreement or arbitral award arising out of a legal relationship, whether contractual or not, which is considered as commercial, including a transaction, contract, or agreement described in [section 2 of the FAA], falls under the Convention [on the Recognition and Enforcement of Foreign Arbitral Awards of June 10, 1958, 21 U.S.T. 2519, T.I.A.S. No. 6997 ("New York Convention")]." 9 U.S.C. § 202. The FAA further provides that "[a]n agreement or award arising out of such a relationship which is entirely between citizens of the United States shall be deemed not to fall under the [New York] Convention unless that relationship involves property located abroad, envisages performance or enforcement abroad, or has some other reasonable relation with one or more foreign states." *Id.* Under Chapter 2, "any party to the arbitration may apply to any court having jurisdiction under this chapter for an order confirming the award as against any other party to the arbitration. The court shall confirm the award unless it finds one of the grounds for refusal or deferral of recognition or enforcement of the award specified in the said [New York] Convention." *Id.* § 207. Chapter 2 further provides that "[t]he district courts of the United States . . . shall have original jurisdiction over . . . an action or proceeding [under the New York Convention], regardless of the amount in controversy." *Id.* § 203.

Chapter 2 also provides that "Chapter 1 applies to actions and proceedings brought under this chapter to the extent that chapter is not in conflict with this chapter or the [New York] Convention as ratified by the United States." *Id.* § 208. Chapter 1, in turn, provides that "[a] written provision in . . . a contract evidencing a transaction involving commerce to settle by arbitration a controversy thereafter arising out of such contract or transaction, or the refusal to perform the whole or any part thereof, or an agreement in writing to submit to arbitration an existing controversy arising out of such a contract, transaction, or refusal, shall be valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract." *Id.* § 2. Chapter 1 further provides that "any party to the arbitration may apply to the court so specified for an order confirming the award, and thereupon the court must grant such an order unless the award is vacated, modified, or corrected as prescribed in sections 10 and 11 of [the FAA]." *Id.* § 9.

Any such cases must be brought in the federal district court whose territorial coverage includes the primary place of business of the Privacy Shield organization.

This arbitration option is intended to resolve individual disputes, and arbitral decisions are not intended to function as persuasive or binding precedent in matters involving other parties, including in future arbitrations or in Swiss, EU or U.S. courts, or FTC proceedings.

F. The Arbitration Panel

The parties will select the arbitrators from the list of arbitrators developed under the EU-U.S. Privacy Shield Framework, as supplemented by a list of arbitrators with European or Swiss expertise to be selected as discussed below.

Consistent with applicable law, the U.S. Department of Commerce and the Swiss Administration will develop a supplemental list of up to 5 arbitrators, chosen on the basis of independence, integrity, and expertise. The following shall apply in connection with this process:

Arbitrators:

(1) will remain on the list for a period of 3 years, absent exceptional circumstances or for cause, renewable for one additional period of 3 years;
(2) shall not be subject to any instructions from, or be affiliated with, either party, or any Privacy Shield organization, or the U.S., Switzerland, EU, or any EU Member State or any other governmental authority, public authority, or enforcement authority; and
(3) must be admitted to practice law in the U.S. and be experts in U.S. privacy law, with expertise in European or Swiss data protection law.

G. Arbitration Procedures

Consistent with applicable law, the Department of Commerce and the Swiss Administration agree to adopt the arbitral procedures adopted under the EU-U.S. Privacy Shield Framework, which includes the following eight considerations, subject to the ninth consideration below:

1. An individual may initiate binding arbitration, subject to the pre-arbitration requirements provision above, by delivering a "Notice" to the organization. The Notice shall contain a summary of steps taken under Paragraph C to resolve the claim, a description of the alleged violation, and, at the choice of the individual, any supporting documents and materials and/or a discussion of law relating to the alleged claim.
2. Procedures will be developed to ensure that an individual's same claimed violation does not receive duplicative remedies or procedures.
3. FTC action may proceed in parallel with arbitration.
4. The location of the arbitration will be the United States, and the individual may choose video or telephone participation, which will be provided at no cost to the individual. In-person participation will not be required.
5. The language of the arbitration will be English unless otherwise agreed by the parties. Upon a reasoned request, and taking into account whether the individual is represented by an attorney, interpretation at the arbitral hearing as well as translation of arbitral materials will

be provided at no cost to the individual, unless the panel finds that, under the circumstances of the specific arbitration, this would lead to unjustified or disproportionate costs.

6. Materials submitted to arbitrators will be treated confidentially and will only be used in connection with the arbitration.
7. Individual-specific discovery may be permitted if necessary, and such discovery will be treated confidentially by the parties and will only be used in connection with the arbitration.
8. Arbitrations should be completed within 90 days of the delivery of the Notice to the organization at issue, unless otherwise agreed to by the parties.
9. No representative of the U.S., EU, Switzerland or any EU Member State or any other governmental authority, public authority, or enforcement authority may participate in these arbitrations, provided, that at the request of a Swiss individual, the Commissioner may provide assistance in the preparation only of the Notice but the Commissioner may not have access to discovery or any other materials related to these arbitrations.

H. Costs

Arbitrators should take reasonable steps to minimize the costs or fees of the arbitrations.

At the annual review, subject to applicable law, the Department of Commerce will take steps to facilitate the establishment of a fund, substantially similar to or the same as the fund established with respect to the EU-U.S. Privacy Shield Framework, into which Privacy Shield organizations will be required to pay an annual contribution, based in part on the size of the organization, which will cover the arbitral cost, including arbitrator fees, up to maximum amounts ("caps"), in consultation with the Swiss Administration. The fund will be managed by a third party, which will report regularly on the operations of the fund. At subsequent annual reviews, the Department of Commerce and Swiss Administration will review the operation of the fund, including the need to adjust the amount of the contributions or of the caps, and will consider, among other things, the number of arbitrations and the costs and timing of the arbitrations, with the mutual understanding that there will be no excessive financial burden imposed on Privacy Shield organizations. Attorney's fees are not covered by this provision or any fund under this provision.

United States Department of State

Under Secretary for Economic Growth, Energy, and the Environment

Washington, D.C. 20520-7512

January 9, 2017

Federal Councillor
Johann N. Schneider-Ammann
Head of the Federal Department of Economic Affairs, Education and Research
Bundeshaus Ost
3003 Bern
Switzerland

Dear Federal Councillor Schneider-Ammann:

I am pleased we reached an understanding on the Swiss-U.S. Privacy Shield, which includes an Ombudsperson Mechanism through which the Swiss Federal Data Protection and Information Commissioner ("FDPIC") may transmit requests on behalf of Swiss individuals regarding U.S. signals intelligence practices.

On January 17, 2014, President Barack Obama announced important intelligence reforms included in Presidential Policy Directive 28 (PPD-28). Under PPD-28, Secretary of State Kerry designated me, the Under Secretary of State for Economic Growth, Energy and the Environment, as the Department's Senior Coordinator for International Information Technology Diplomacy to serve as a point of contact for foreign governments that wish to raise concerns regarding U.S. signals intelligence activities. Building on this role, I was designated to serve as the Ombudsperson in the context of the EU-U.S. Privacy Shield Framework Ombudsperson Mechanism. The Ombudsperson Mechanism is now being extended to the Swiss-U.S. Privacy Shield Framework, in accordance with the terms set out in Annex A thereof. I am independent from the U.S. intelligence community and report directly to the Secretary of State. I am confident the Ombudsperson Mechanism will be an effective means to address Swiss individuals' concerns.

Sincerely,

Catherine A. Novelli

Catherine A. Novelli

ANNEX A:
Swiss-U.S. Privacy Shield
Ombudsperson Mechanism

SWISS-U.S. PRIVACY SHIELD OMBUDSPERSON MECHANISM REGARDING SIGNALS INTELLIGENCE

In recognition of the importance of the Swiss-U.S. Privacy Shield Framework, this Memorandum sets forth the process for implementing a mechanism, consistent with Presidential Policy Directive 28 (PPD-28), regarding signals intelligence.

On January 17, 2014, President Obama gave a speech announcing important intelligence reforms. In that speech, he pointed out that "[o]ur efforts help protect not only our nation, but our friends and allies as well. Our efforts will only be effective if ordinary citizens in other countries have confidence that the United States respects their privacy too." President Obama announced the issuance of a new presidential directive—PPD-28—to "clearly prescribe what we do, and do not do, when it comes to our overseas surveillance."

Section 4(d) of PPD-28 directs the Secretary of State to designate a "Senior Coordinator for International Information Technology Diplomacy" (Senior Coordinator) "to … serve as a point of contact for foreign governments who wish to raise concerns regarding signals intelligence activities conducted by the United States." As of January 2015, Under Secretary C. Novelli has served as the Senior Coordinator.

This Memorandum describes a mechanism that the Senior Coordinator will follow to facilitate the processing of requests relating to national security access to data transmitted from Switzerland to the United States pursuant to the Privacy Shield, standard contractual clauses (SCCs), binding corporate rules (BCRs), "Derogations,"[1] or "Possible Future Derogations,"[2] through established avenues under applicable United States laws and policy, and the response to those requests.

[1] "Derogations" in this context mean a commercial transfer or transfers that take place on the condition that: (a) the data subject has given his consent unambiguously to the proposed transfer; or (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims; or (e) the transfer is necessary in order to protect the vital interests of the data subject; or (f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

[2] "Possible Future Derogations" in this context mean a commercial transfer or transfers that take place on one of the following conditions, to the extent the condition constitutes lawful grounds for transfers of personal data from Switzerland to the U.S.: (a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards; or (b) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or (c) in case of a transfer to a third country or an international organization and none of the other derogations or possible future derogations is applicable, only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data.

1. **The Privacy Shield Ombudsperson.** The Senior Coordinator will serve as the Privacy Shield Ombudsperson and designate additional State Department officials, as appropriate to assist in her performance of the responsibilities detailed in this memorandum. (Hereinafter, the Coordinator and any officials performing such duties will be referred to as "Privacy Shield Ombudsperson.") The Privacy Shield Ombudsperson will work closely with appropriate officials from other departments and agencies who are responsible for processing requests in accordance with applicable United States law and policy. The Ombudsperson is independent from the Intelligence Community. The Ombudsperson reports directly to the Secretary of State who will ensure that the Ombudsperson carries out its function objectively and free from improper influence that is liable to have an effect on the response to be provided.

2. **Effective Coordination.** The Privacy Shield Ombudsperson will be able to effectively use and coordinate with the oversight bodies, described below, in order to ensure that the Ombudsperson's response to requests submitted on behalf of Swiss individuals by the Swiss Federal Data Protection and Information Commissioner ("FDPIC") is based on the necessary information. When the request relates to the compatibility of surveillance with U.S. law, the Privacy Shield Ombudsperson will be able to cooperate with one of the independent oversight bodies with investigatory powers.

    a. The Privacy Shield Ombudsperson will work closely with other United States Government officials, including appropriate independent oversight bodies, to ensure that completed requests are processed and resolved in accordance with applicable laws and policies. In particular, the Privacy Shield Ombudsperson will be able to coordinate closely with the Office of the Director of National Intelligence, the Department of Justice, and other departments and agencies involved in United States national security as appropriate, and Inspectors General, Freedom of Information Act Officers, and Civil Liberties and Privacy Officers.

    b. The United States Government will rely on mechanisms for coordinating and overseeing national security matters across departments and agencies to help ensure that the Privacy Shield Ombudsperson is able to respond within the meaning of Section 4(e) to completed requests under Section 3(b).

    c. The Privacy Shield Ombudsperson may refer matters related to requests to the Privacy and Civil Liberties Oversight Board for its consideration.

3. **Submitting Requests.**

    a. Individuals seeking review under the Ombudsperson Mechanism will submit requests to the FDPIC.
    b. The FDPIC will ensure, in compliance with the following actions, that each request is complete before submitting it to the Privacy Shield Ombudsperson:

(i) Verifying the identity of the individual, and that the individual is acting on his/her own behalf, and not as a representative of a governmental or intergovernmental organization.

(ii) Ensuring the request is made in writing, and that it contains the following basic information:

- any information that forms the basis for the request,
- the nature of information or relief sought,
- the United States Government entities believed to be involved, if any, and
- the other measures pursued to obtain the information or relief requested and the response received through those other measures.

(iii) Verifying that the request pertains to data reasonably believed to have been transferred from Switzerland to the United States pursuant to the Privacy Shield, SCCs, BCRs, Derogations, or Possible Future Derogations.

(iv) Making an initial determination that the request is not frivolous, vexatious, or made in bad faith.

c. To be completed for purposes of further handling by the Privacy Shield Ombudsperson under this memorandum, the request need not demonstrate that the requester's data has in fact been accessed by the United States Government through signal intelligence activities.

4. **Commitments to Communicate with FDPIC**.

a. The Privacy Shield Ombudsperson will acknowledge receipt of the request to the FDPIC.

b. The Privacy Shield Ombudsperson will conduct an initial review to verify that the request has been completed in conformance with Section 3(b). If the Privacy Shield Ombudsperson notes any deficiencies or has any questions regarding the completion of the request, the Privacy Shield Ombudsperson will seek to address and resolve those concerns with the FDPIC.

c. If, to facilitate appropriate processing of the request, the Privacy Shield Ombudsperson needs more information about the request, or if specific action is needed to be taken by the individual who originally submitted the request, the Privacy Shield Ombudsperson will so inform the FDPIC.

d. The Privacy Shield Ombudsperson will track the status of requests and provide updates as appropriate to the FDPIC.

e. Once a request has been completed as described in Section 3 of this Memorandum, the Privacy Shield Ombudsperson will provide in a timely manner an appropriate response to the FDPIC , subject to the continuing obligation to protect information under applicable laws and policies. The Privacy Shield Ombudsperson will provide a response to the

FDPIC confirming (i) that the complaint has been properly investigated, and (ii) that the U.S. law, statutes, executives orders, presidential directives, and agency policies, providing the limitations and safeguards described in the ODNI letter, have been complied with, or, in the event of non-compliance, such non-compliance has been remedied. The Privacy Shield Ombudsperson will neither confirm nor deny whether the individual has been the target of surveillance nor will the Privacy Shield Ombudsperson confirm the specific remedy that was applied. As further explained in Section 5, FOIA requests will be processed as provided under that statute and applicable regulations.

f. The Privacy Shield Ombudsperson will communicate directly with the FDPIC, who will in turn be responsible for communicating with the individual submitting the request. If direct communications are part of one of the underlying processes described below, then those communications will take place in accordance with existing procedures.

g. Commitments in this Memorandum will not apply to general claims that the Swiss-U.S. Privacy Shield is inconsistent with Swiss data protection requirements. The commitments in this Memorandum are made based on the common understanding by the Swiss government and the U.S. government that given the scope of commitments under this mechanism, there may be resource constraints that arise, including with respect to Freedom of Information Act (FOIA) requests. Should the carrying-out of the Privacy Shield Ombudsperson's functions exceed reasonable resource constraints and impede the fulfillment of these commitments, the U.S. government will discuss with the Swiss government any adjustments that may be appropriate to address the situation.

5. **Requests for Information.** Requests for access to U. S. government records may be made and processed under the Freedom of Information Act (FOIA).

a. FOIA provides a means for any person to seek access to existing federal agency records, regardless of the nationality of the requester. This statute is codified in the United States Code at 5 U.S.C. § 552. The statute, together with additional information about FOIA, is available at www.FOIA.gov and http://www.justice.gov/oip/foia-resources. Each agency has a Chief FOIA Officer, and has provided information on its public website about how to submit a FOIA request to the agency. Agencies have processes for consulting with one another on FOIA requests that involve records held by another agency.

b. By way of example:

(i) The Office of the Director of National Intelligence (ODNI) has established the ODNI FOIA Portal for the ODNI: http://www.dni.gov/index.php/about-this-site/foia. This portal provides information on submitting a request, checking on the status of an existing request, and accessing information that has been released and published by the ODNI under FOIA. The ODNI FOIA Portal includes links to other FOIA websites for IC elements: http://www.dni.gov/index.php/about-this-site/foia/other-ic-foia-sites.

(ii) The Department of Justice's Office of Information Policy provides comprehensive information about FOIA: http://www.justice.gov/oip. This includes not only information about submitting a FOIA request to the Department of Justice, but also provides guidance to the United States government on interpreting and applying FOIA requirements.

c. Under FOIA, access to government records is subject to certain enumerated exemptions. These include limits on access to classified national security information, personal information of third parties, and information concerning law enforcement investigations, and are comparable to the limitations imposed by Swiss legal provisions on information access. These limitations apply equally to Americans and non-Americans.

d. Disputes over the release of records requested pursuant to FOIA can be appealed administratively and then in federal court. The court is required to make a *de novo* determination of whether records are properly withheld, 5 U.S.C. § 552(a)(4)(B), and can compel the government to provide access to records. In some cases courts have overturned government assertions that information should be withheld as classified. Although no monetary damages are available, courts can award attorney's fees.

6. **Requests for Further Action.** A request alleging violation of law or other misconduct will be referred to the appropriate U. S. government body, including independent oversight bodies, with the power to investigate the respective request and address non-compliance as described below.

a. Inspectors General are statutorily independent; have broad power to conduct investigations, audits and reviews of programs, including of fraud and abuse or violation of law; and can recommend corrective actions.

(i) The Inspector General Act of 1978, as amended, statutorily established the Federal Inspectors General (IG) as independent and objective units within most agencies whose duties are to combat waste, fraud, and abuse in the programs and operations of their respective agencies. To this end, each IG is responsible for conducting audits and investigations relating to the programs and operations of its agency. Additionally, IGs provide leadership and coordination and recommend policies for activities designed to promote economy, efficiency, and effectiveness, and prevent and detect fraud and abuse, in agency programs and operations.

(ii) Each element of the Intelligence Community has its own Office of the Inspector General with responsibility for oversight of foreign intelligence activities, among other matters. A number of Inspector General reports about intelligence programs have been publicly released.

(iii) By way of example:

- The Office of the Inspector General of the Intelligence Community (IC IG) was established pursuant to Section 405 of the Intelligence Authorization Act of Fiscal Year 2010. The IC IG is responsible for conducting IC-wide audits, investigations, inspections, and reviews that identify and address systemic risks, vulnerabilities, and deficiencies that cut across IC agency missions, in order to positively impact IC-wide economies and efficiencies. The IC IG is authorized to investigate complaints or information concerning allegations of a violation of law, rule, regulation, waste, fraud, abuse of authority, or a substantial or specific danger to public health and safety in connection with ODNI and/or IC intelligence programs and activities. The IC IG provides information on how to contact the IC IG directly to submit a report: http://www.dni.gov/index.php/about-this-site/contact-the-ig.

- The Office of the Inspector General (OIG) in the U.S. Department of Justice (DOJ) is a statutorily created independent entity whose mission is to detect and deter waste, fraud, abuse, and misconduct in DOJ programs and personnel, and to promote economy and efficiency in those programs. The OIG investigates alleged violations of criminal and civil laws by DOJ employees and also audits and inspects DOJ programs. The OIG has jurisdiction over all complaints of misconduct against Department of Justice employees, including the Federal Bureau of Investigation; Drug Enforcement Administration; Federal Bureau of Prisons; U.S. Marshals Service; Bureau of Alcohol, Tobacco, Firearms, and Explosives; United States Attorneys Offices; and employees who work in other Divisions or Offices in the Department of Justice. (The one exception is that allegations of misconduct by a Department attorney or law enforcement personnel that relate to the exercise of the Department attorney's authority to investigate, litigate, or provide legal advice are the responsibility of the Department's Office of Professional Responsibility.) In addition, section 1001 of the USA Patriot Act, signed into law on October 26, 2001, directs the Inspector General to review information and receive complaints alleging abuses of civil rights and civil liberties by Department of Justice employees. The OIG maintains a public website – https://www.oig.justice.gov – which includes a "Hotline" for submitting complaints – https://www.oig.justice.gov/hotline/index.htm.

b. Privacy and Civil Liberties offices and entities in the United States Government also have relevant responsibilities. By way of example:

(i) Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, codified in the United States Code at 42 U.S.C. § 2000-ee1, establishes privacy and civil liberties officers at certain departments and agencies (including the Department of State, Department of Justice, and ODNI). Section 803 specifies that these privacy and civil liberties officers will serve as the principal advisor to, among

other things, ensure that such department, agency, or element has adequate procedures to address complaints from individuals who allege such department, agency, or element has violated their privacy or civil liberties.

(ii) The ODNI's Civil Liberties and Privacy Office (ODNI CLPO) is led by the ODNI Civil Liberties Protection Officer, a position established by the National Security Act of 1948, as amended. The duties of the ODNI CLPO include ensuring that the policies and procedures of the elements of the Intelligence Community include adequate protections for privacy and civil liberties, and reviewing and investigating complaints alleging abuse or violation of civil liberties and privacy in ODNI programs and activities. The ODNI CLPO provides information to the public on its website, including instructions for how to submit a complaint: www.dni.gov/clpo. If the ODNI CLPO receives a privacy or civil liberties complaint involving IC programs and activities, it will coordinate with other IC elements on how that complaint should be further processed within the IC. Note that the National Security Agency (NSA) also has a Civil Liberties and Privacy Office, which provides information about its responsibilities on its website – https://www.nsa.gov/civil_liberties/. If information indicates that an agency is out of compliance with privacy requirements (*e.g.*, a requirement under Section 4 of PPD-28), then agencies have compliance mechanisms to review and remedy the incident. Agencies are required to report compliance incidents under PPD-28 to the ODNI.

(iii) The Office of Privacy and Civil Liberties (OPCL) at the Department of Justice supports the duties and responsibilities of the Department's Chief Privacy and Civil Liberties Officer (CPCLO). The principal mission of OPCL is to protect the privacy and civil liberties of the American people through review, oversight, and coordination of the Department's privacy operations. OPCL provides legal advice and guidance to Departmental components; ensures the Department's privacy compliance, including compliance with the Privacy Act of 1974, the privacy provisions of both the E-Government Act of 2002 and the Federal Information Security Management Act, as well as administration policy directives issued in furtherance of those Acts; develops and provides Departmental privacy training; assists the CPCLO in developing Departmental privacy policy; prepares privacy-related reporting to the President and Congress; and reviews the information handling practices of the Department to ensure that such practices are consistent with the protection of privacy and civil liberties. OPCL provides information to the public about its responsibilities at http://www.justice.gov/opcl.

(iv) According to 42 U.S.C. § 2000ee *et seq.*, the Privacy and Civil Liberties Oversight Board shall continually review (i) the policies and procedures, as well as their implementation, of the departments, agencies and elements of the executive branch relating to efforts to protect the Nation from terrorism to ensure that privacy and civil liberties are protected, and (ii) other actions by the executive branch relating to

such efforts to determine whether such actions appropriately protect privacy and civil liberties and are consistent with governing laws, regulations, and policies regarding privacy and civil liberties. It shall receive and review reports and other information from privacy officers and civil liberties officers and, when appropriate, make recommendations to them regarding their activities. Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, codified at 42 U.S.C. § 2000ee-1, directs the privacy and civil liberties officers of eight federal agencies (including the Secretary of Defense, Secretary of Homeland Security, Director of National Intelligence, and Director of the Central Intelligence Agency), and any additional agency designated by the Board, to submit periodic reports to the PCLOB, including the number, nature, and disposition of the complaints received by the respective agency for alleged violations. The PCLOB's enabling statute directs the Board to receive these reports and, when appropriate, make recommendations to the privacy and civil liberties officers regarding their activities.

United States of America
FEDERAL TRADE COMMISSION
WASHINGTON, DC 20580

OFFICE OF CHAIRWOMAN
EDITH RAMIREZ

January 9, 2017

VIA EMAIL

Federal Councillor
Johann N. Schneider-Ammann
Head of the Department of Economic Affairs, Education and Research
Bundeshaus Ost
3003 Bern
Switzerland

Dear Federal Councillor:

I appreciate this opportunity to affirm the Federal Trade Commission's commitment to enforce the Swiss-U.S. Privacy Shield Framework, which is modeled on the EU-US Privacy Shield Framework and replaces the U.S.-Swiss Safe Harbor Framework. We believe this new Framework will facilitate continued trade between the United States and Switzerland and strengthen privacy protections for Swiss consumers.

I have previously explained the FTC's commitment to enforce the EU-U.S. Privacy Shield in correspondence to Věra Jourová, the European Union's Commissioner for Justice, Consumers and Gender Equality,[1] and extend these same assurances in connection with the Swiss-U.S. Privacy Shield Framework. In particular, I want to highlight the FTC's commitment in four key areas: (1) referral prioritization and investigations; (2) addressing false or deceptive Privacy Shield membership claims; (3) continued order monitoring; and (4) enhanced engagement and enforcement cooperation. We provide below detailed information about each of these, together with relevant background about the FTC's role in protecting consumer privacy and enforcing the Safe Harbor programs.[2]

---

[1] *See* Letter from Edith Ramirez, Chairwoman, Fed. Trade Comm'n, to Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission (July 7, 2016), *available at* https://www.ftc.gov/public-statements/2016/07/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice [hereinafter FTC EU-U.S. Privacy Shield Letter].

[2] Additional information about FTC privacy enforcement and policy work and U.S. federal and state privacy laws is provided in the FTC EU-U.S. Privacy Shield Letter, including in Attachment A. In addition, a summary of our recent privacy and security enforcement actions is available on the FTC's website at https://www.ftc.gov/reports/privacy-data-security-update-2015.

I. Background

A. FTC Privacy Enforcement and Policy Work

The FTC has broad civil enforcement authority to promote consumer protection and competition in the commercial sphere. As part of its consumer protection mandate, the FTC enforces a wide range of laws to protect the privacy and security of consumer data. The primary law enforced by the FTC, the FTC Act, prohibits "unfair" and "deceptive" acts or practices in or affecting commerce.[3] A representation, omission, or practice is deceptive if it is material and likely to mislead consumers acting reasonably under the circumstances.[4] An act or practice is unfair if it causes, or is likely to cause, substantial injury that is not reasonably avoidable by consumers or outweighed by countervailing benefits to consumers or competition.[5] The FTC also enforces targeted statutes that protect information relating to health, credit, and other financial matters, as well as children's online information, and has issued regulations implementing each of these statutes.

The FTC's jurisdiction under the FTC Act applies to matters "in or affecting commerce." The FTC does not have jurisdiction over criminal law enforcement or national security matters. Nor can the FTC reach most other governmental actions. In addition, there are exceptions to the FTC's jurisdiction over commercial activities, including with respect to banks, airlines, the business of insurance, and the common carrier activities of telecommunications service providers.[6] The FTC also does not have jurisdiction over most non-profit organizations, but it does have jurisdiction over sham charities or other non-profits that in actuality operate for profit. The FTC also has jurisdiction over non-profit organizations that operate for the profit of their for-profit members, including by providing substantial economic benefits to those members.[7] In some instances, the FTC's jurisdiction is concurrent with that of other law enforcement agencies. We have developed strong working relationships with federal and state authorities and work closely with them to coordinate investigations or make referrals where appropriate.

Enforcement is the lynchpin of the FTC's approach to privacy protection. To date, the FTC has brought over 500 cases protecting the privacy and security of consumer information. This body of cases covers both offline and online information and includes enforcement actions against companies large and small, alleging that they failed to properly dispose of sensitive consumer data, failed to secure consumers' personal information, deceptively tracked consumers online, spammed consumers, installed spyware or other malware on consumers' computers, violated Do Not Call and other telemarketing rules, and improperly collected and shared consumer information on mobile devices. The FTC's enforcement actions – in both the physical

---

[3] 15 U.S.C. § 45(a).
[4] *See* FTC Policy Statement on Deception, *appended to Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984), *available at* https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.
[5] *See* 15 U.S.C § 45(n); FTC Policy Statement on Unfairness, *appended to Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984), *available at* https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.
[6] The FTC's longstanding view is that it has jurisdiction over the non-common carrier activities of common carriers. This issue is currently being litigated.
[7] *See California Dental Ass'n v. FTC*, 526 U.S. 756 (1999).

and digital worlds – send an important message to companies about the need to protect consumer privacy.

Our enforcement actions also have a global impact. The FTC Act's prohibition on unfair or deceptive acts or practices is not limited to protecting U.S. consumers from U.S. companies, as it includes those practices that (1) cause or are likely to cause reasonably foreseeable injury in the United States, or (2) involve material conduct in the United States. Further, the FTC can use all remedies, including restitution, that are available to protect domestic consumers when protecting foreign consumers.

Our cases enforcing Section 5 of the FTC Act have protected the privacy of U.S. and foreign consumers alike. For example, in a case against an information broker, Accusearch, the FTC alleged that the company's sale of confidential telephone records to third parties without consumers' knowledge or consent was an unfair practice in violation of Section 5 of the FTC Act. Accusearch sold information relating to both U.S. and foreign consumers.[8] The court granted injunctive relief against Accusearch prohibiting, among other things, the marketing or sale of consumers' personal information without written consent, unless it was lawfully obtained from publicly available information, and ordered disgorgement of almost $200,000.[9]

Another notable case is our recent action against the Canadian operators of the dating website AshleyMadison.com, in which we alleged, among other things, that the site operators failed to take reasonable steps to secure their users' personal information, resulting in the unauthorized disclosure of sensitive information about 36 million consumers worldwide.[10] This case not only demonstrates the FTC's authority to take action to address cross-border privacy and security law violations but also highlights how effective cooperation with foreign privacy authorities enhances our ability to protect consumers from harmful privacy and security practices that have global implications. Our cooperation with the Canadian and Australian privacy authorities in this case helped us obtain more comprehensive information and investigate the security practices more efficiently, as well as facilitated our collective efforts to protect consumers in countries around the world.

In addition to its enforcement work, the FTC has also pursued numerous policy initiatives aimed at enhancing consumer privacy. The FTC has hosted workshops and issued reports recommending best practices aimed at improving privacy in the mobile ecosystem; increasing transparency of the data broker industry; maximizing the benefits of big data while mitigating its risks, particularly for low-income and underserved consumers; and highlighting the privacy and security implications of facial recognition and the Internet of Things, among other areas. Most recently, the FTC's Fall Technology Series has examined the privacy and security implications of ransomware, drones, and smart entertainment devices.

---

[8] *See* Office of the Privacy Commissioner of Canada, Complaint under PIPEDA against Accusearch, Inc., doing business as Abika.com, https://www.priv.gc.ca/cf-dc/2009/2009_009_0731_e.asp. The Office of the Privacy Commissioner of Canada filed an *amicus curiae* brief in the appeal of the FTC action and conducted its own investigation, concluding that Accusearch's practices also violated Canadian law.

[9] *See FTC v. Accusearch, Inc.*, No. 06CV015D (D. Wyo. Dec. 20, 2007), *aff'd* 570 F.3d 1187 (10th Cir. 2009).

[10] *See FTC v. Ruby Corp.*, No. 1:16-cv-02438 (D.D.C. Dec. 14, 2016).

B. Safe Harbor Enforcement

As part of its robust privacy and security enforcement program, the FTC has sought to protect Swiss and EU consumers by bringing enforcement actions that involved Safe Harbor violations. The FTC has brought 39 Safe Harbor enforcement actions: 36 alleging false certification claims, and three cases—against Google, Facebook, and Myspace—involving alleged violations of Safe Harbor Privacy Principles.[11] Ten of these cases involved the U.S.-Swiss Safe Harbor.[12] These cases demonstrate the enforceability of certifications and the repercussions for non-compliance. Twenty-year consent orders require Google, Facebook, and Myspace to implement comprehensive privacy programs that must be reasonably designed to address privacy risks related to the development and management of new and existing products and services and to protect the privacy and confidentiality of personal information. The comprehensive privacy programs mandated under these orders must identify foreseeable material risks and have controls to address those risks. The companies must also submit to ongoing, independent assessments of their privacy programs, which must be provided to the FTC. The orders also prohibit these companies from misrepresenting their privacy practices and their participation in any privacy or security program. This prohibition would also apply to companies' acts and practices under the new EU-U.S. and Swiss-U.S. Privacy Shield Frameworks. The FTC can enforce these orders by seeking civil penalties. In fact, Google paid a record $22.5 million civil penalty in 2012 to resolve allegations it had violated its order. Consequently, these FTC orders help protect over a billion consumers worldwide, hundreds of millions of whom reside in Europe.

Many of our other Safe Harbor enforcement cases involved organizations that joined the Safe Harbor program but failed to renew their annual certification while they continued to represent themselves as current members. As discussed further below, the FTC also commits to addressing false claims of participation in the Privacy Shield Framework. This strategic enforcement activity will complement the Department of Commerce's increased actions to verify compliance with program requirements for certification and re-certification, its monitoring of

---

[11] *See In the Matter of Google, Inc.,* No. C-4336 (F.T.C. Oct. 13 2011) (decision and order), *available at* https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz; *In the Matter of Facebook, Inc.*, No. C-4365 (F.T.C. July 27, 2012) (decision and order), *available at* https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook; *In the Matter of Myspace LLC*, No. C-4369 (F.T.C. Aug. 30, 2012) (decision and order), *available at* https://www.ftc.gov/news-events/press-releases/2012/09/ftc-finalizes-privacy-settlement-myspace.

[12] *See* Press Release, Fed. Trade Comm'n, Thirteen Companies Agree to Settle FTC Charges They Falsely Claimed to Comply with International Safe Harbor Framework (Aug. 17, 2015), *available at* https://www.ftc.gov/news-events/press-releases/2015/08/thirteen-companies-agree-settle-ftc-charges-they-falsely-claimed (Just Bagels Manufacturing, Inc.; Pinger, Inc.; NAICS Association, LLC; Golf Connect, LLC); Press Release, Fed. Trade Comm'n, FTC Settles with Two Companies Falsely Claiming to Comply with International Safe Harbor Framework (April 7, 2015), *available at* https://www.ftc.gov/news-events/press-releases/2015/04/ftc-settles-two-companies-falsely-claiming-comply-international (TES Franchising, LLC); Press Release, Fed. Trade Comm'n, FTC Approves Final Orders Settling Charges of U.S.-EU Safe Harbor Violations Against 14 Companies (June 25, 2014), *available at* https://www.ftc.gov/news-events/press-releases/2014/06/ftc-approves-final-orders-settling-charges-us-eu-safe-harbor (American Apparel, Inc.; Apperian, Inc.; Level 3 Communications, LLC; DataMotion, Inc.); *In the Matter of Myspace LLC*, No. C-4369 (F.T.C. Aug. 30, 2012) (decision and order), *available at* https://www.ftc.gov/news-events/press-releases/2012/09/ftc-finalizes-privacy-settlement-myspace.

effective compliance, including through the use of questionnaires to Framework participants, and its increased efforts to identify false Framework membership claims and misuse of any Framework certification mark.[13]

II. Referral Prioritization and Investigations

As we did under the Safe Harbor program, the FTC commits to give priority to Privacy Shield referrals from the Swiss Federal Data Protection and Information Commissioner ("Swiss DPA"). We will also prioritize referrals of non-compliance with self-regulatory guidelines relating to the Privacy Shield Framework from privacy self-regulatory organizations and other independent dispute resolution bodies.

To facilitate referrals under the Framework from Switzerland, the FTC is creating a standardized referral process and providing guidance to the Swiss DPA on the type of information that would best assist the FTC in its inquiry into a referral. As part of this effort, the FTC will designate an agency point of contact for Swiss DPA referrals. It is most useful when the referring authority has conducted a preliminary inquiry into the alleged violation and can cooperate with the FTC in an investigation.

Upon receipt of a referral from the Swiss DPA or a self-regulatory organization, the FTC can take a range of actions to address the issues raised. For example, we may review the company's privacy policies, obtain further information directly from the company or from third parties, follow up with the referring entity, assess whether there is a pattern of violations or significant number of consumers affected, determine whether the referral implicates issues within the purview of the Department of Commerce, assess whether consumer and business education would be helpful, and, as appropriate, initiate an enforcement proceeding.

The FTC also commits to exchange information on referrals with the Swiss DPA, including the status of referrals, subject to confidentiality laws and restrictions. To the extent feasible given the number and type of referrals received, the information provided will include an evaluation of the referred matters, including a description of significant issues raised and any action taken to address law violations within the jurisdiction of the FTC. The FTC will also provide feedback to the Swiss DPA on the types of referrals received in order to increase the effectiveness of efforts to address unlawful conduct. If the Swiss DPA seeks information about the status of a particular referral for purposes of pursuing its own enforcement proceeding, the FTC will respond, taking into account the number of referrals under consideration and subject to confidentiality and other legal requirements.

The FTC will also work closely with the Swiss DPA to provide enforcement assistance. In appropriate cases, this could include information sharing and investigative assistance pursuant to the U.S. SAFE WEB Act, which authorizes FTC assistance to foreign law enforcement agencies when the foreign agency is enforcing laws prohibiting practices that are substantially

[13] Letter from Ken Hyatt, Acting Under Secretary of Commerce for International Trade, International Trade Administration, to Federal Councillor Johann N. Schneider-Ammann, Head of the Department of Economic Affairs, Education and Research (Jan. 9, 2017).

similar to those prohibited by laws the FTC enforces.[14] As part of this assistance, the FTC can share information obtained in connection with an FTC investigation, issue compulsory process on behalf of the Swiss DPA conducting its own investigation, and seek oral testimony from witnesses or defendants in connection with the DPA's enforcement proceeding, subject to the requirements of the U.S. SAFE WEB Act. The FTC regularly uses this authority to assist other authorities around the world in privacy and consumer protection cases.[15]

In addition to prioritizing Privacy Shield referrals from the Swiss DPA and privacy self-regulatory organizations,[16] the FTC commits to investigating possible Framework violations on its own initiative where appropriate using a range of tools.

For well over a decade, the FTC has maintained a robust program of investigating privacy and security issues involving commercial organizations. As part of these investigations, the FTC routinely examined whether the entity at issue was making Safe Harbor representations. If the entity was making such representations and the investigation revealed apparent violations of the Safe Harbor Privacy Principles, the FTC included allegations of Safe Harbor violations in its enforcement actions. We will continue this proactive approach under the new Framework. Importantly, the FTC conducts many more investigations than ultimately result in public enforcement actions. Many FTC investigations are closed because staff does not identify an apparent law violation. Because FTC investigations are non-public and confidential, the closing of an investigation is often not made public.

The nearly 40 enforcement actions initiated by the FTC involving the U.S.-EU and U.S.-Swiss Safe Harbor programs evidence the agency's commitment to proactive enforcement of cross-border privacy programs. The FTC will look for potential Framework violations as part of the privacy and security investigations we undertake on a regular basis.

---

[14] In determining whether to exercise its U.S. SAFE WEB Act authority, the FTC considers, *inter alia*: "(A) whether the requesting agency has agreed to provide or will provide reciprocal assistance to the Commission; (B) whether compliance with the request would prejudice the public interest of the United States; and (C) whether the requesting agency's investigation or enforcement proceeding concerns acts or practices that cause or are likely to cause injury to a significant number of persons." 15 U.S.C. § 46(j)(3). This authority does not apply to enforcement of competition laws.

[15] In fiscal years 2012-2015, for example, the FTC used its U.S. SAFE WEB Act authority to share information in response to almost 60 requests from foreign agencies and it issued nearly 60 civil investigative demands (equivalent to administrative subpoenas) to aid 25 foreign investigations.

[16] Although the FTC does not resolve or mediate individual consumer complaints, the FTC affirms that it will prioritize Privacy Shield referrals from the Swiss DPA. In addition, the FTC uses complaints in its Consumer Sentinel database, which is accessible by many other law enforcement agencies, to identify trends, determine enforcement priorities, and identify potential investigative targets. Swiss individuals can use the same complaint system available to U.S. consumers to submit a complaint to the FTC at www.ftc.gov/complaint. For individual Privacy Shield complaints, however, it may be most useful for Swiss individuals to submit complaints to the Swiss DPA or an alternative dispute resolution provider.

III. Addressing False or Deceptive Privacy Shield Membership Claims

As referenced above, the FTC will take action against entities that misrepresent their participation in the Framework. The FTC will give priority consideration to referrals from the Department of Commerce regarding organizations that it identifies as improperly holding themselves out to be current members of the Framework or using any Framework certification mark without authorization.

In addition, we note that if an organization's privacy policy promises that it complies with the Privacy Shield Principles, its failure to make or maintain a registration with the Department of Commerce likely will not, by itself, excuse the organization from FTC enforcement of those Framework commitments.

IV. Order Monitoring

The FTC also affirms its commitment to monitor enforcement orders to ensure compliance with the Privacy Shield Framework.

We will require compliance with the Framework through a variety of appropriate injunctive provisions in future FTC Framework orders. This includes prohibiting misrepresentations regarding the Framework and other privacy programs when these are the basis for the underlying FTC action.

The FTC's cases enforcing the original Safe Harbor program are instructive. In the 36 cases involving false or deceptive claims of Safe Harbor certification, each order prohibits the defendant from misrepresenting its participation in Safe Harbor or any other privacy or security program and requires the company to make compliance reports available to the FTC. In cases that involved violations of Safe Harbor Privacy Principles, companies have been required to implement comprehensive privacy programs and obtain independent third-party assessments of those programs every other year for twenty years, which they must provide to the FTC.

Violations of the FTC's administrative orders can lead to civil penalties of up to $40,000 per violation, or $40,000 per day for a continuing violation,[17] which, in the case of practices affecting many consumers, can amount to millions of dollars. Each consent order also has reporting and compliance provisions. The entities under order must retain documents demonstrating their compliance for a specified number of years. The orders must also be disseminated to employees responsible for ensuring order compliance.

The FTC systematically monitors compliance with Safe Harbor orders, as it does with all of its orders. The FTC takes enforcement of its privacy and data security orders seriously and brings actions to enforce them when necessary. For example, as noted above, Google paid a $22.5 million civil penalty to resolve allegations it had violated its FTC order. Importantly, FTC orders will continue to protect all consumers worldwide who interact with a business, not just those consumers who have lodged complaints.

[17] 15 U.S.C. § 45(m); 16 C.F.R. § 1.98.

Finally, the FTC will continue to maintain an online list of companies subject to orders obtained in connection with enforcement of both the Safe Harbor program and the new Privacy Shield Framework.[18] In addition, the Privacy Shield Principles now require companies subject to an FTC or court order based on non-compliance with the Principles to make public any relevant Framework-related sections of any compliance or assessment report submitted to the FTC, to the extent consistent with confidentiality laws and rules.

V. Engagement With the Swiss DPA and Enforcement Cooperation

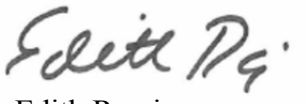
The FTC recognizes the important role that the Swiss DPA plays with respect to Framework compliance, and encourages increased consultation and enforcement cooperation. In addition to any consultation with the Swiss DPA on referral-specific matters, the FTC commits to participate in periodic meetings with the Swiss DPA to discuss in general terms how to improve enforcement cooperation with respect to the Framework. The FTC will also participate in the annual review of the Framework to discuss its implementation.

The FTC also encourages the development of tools that will enhance enforcement cooperation with the Swiss DPA, as well as other privacy enforcement authorities around the world. In particular, the FTC, along with enforcement partners in the European Union and around the globe, last year launched an alert system within the Global Privacy Enforcement Network ("GPEN") to share information about investigations and promote enforcement coordination. This GPEN Alert tool could be particularly useful in the context of the Privacy Shield Framework. The FTC and the Swiss DPA could use it to coordinate with respect to the Framework and other privacy investigations, including as a starting point for sharing information in order to deliver coordinated and more effective privacy protection for consumers. We look forward to continuing to work with participating authorities to deploy the GPEN Alert system more broadly and develop other tools to improve enforcement cooperation in privacy cases, including those involving the Framework.

***

The FTC is pleased to affirm its commitment to enforcing the new Privacy Shield Framework. We also look forward to continuing engagement with our Swiss colleagues as we work together to protect consumer privacy.

Sincerely,



Edith Ramirez
Chairwoman

[18] *See* FTC, Business Center, Legal Resources, https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field_consumer_protection_topics_tid=251.

THE SECRETARY OF TRANSPORTATION
WASHINGTON, DC 20590

January 9, 2017

Mr. Johann N. Schneider-Ammann
Federal Councillor
Head of the Department of Economic Affairs,
Education and Research
Bundeshaus Ost
3003 Bern
THE SWISS CONFEDERATION

Re: Swiss-U.S. Privacy Shield Framework

Dear Councillor Schneider-Ammann:

The United States Department of Transportation ("Department" or "DOT") appreciates the opportunity to describe its role in enforcing the Swiss-U.S. Privacy Shield Framework (Privacy Shield). Privacy Shield plays a critical role in protecting personal data provided during commercial transactions in an increasingly interconnected world. It enables businesses to conduct important operations in the global economy, while at the same time ensuring that Swiss consumers retain important privacy protections.

The DOT first publicly expressed its commitment to enforcement of the Swiss-U.S. Safe Harbor Framework in a letter sent to the Federal Data Protection and Information Commissioner in November 2008. The DOT pledged to vigorously enforce the Safe Harbor Privacy Principles in that letter. The DOT continues to uphold this commitment and this letter memorializes that commitment.

Notably, DOT renews its commitment in the following key areas: (1) prioritization of investigation of alleged Privacy Shield violations; (2) appropriate enforcement action against entities making false or deceptive Privacy Shield certification claims; and (3) monitoring and making public enforcement orders concerning Privacy Shield violations. We provide information about each of these commitments and, for necessary context, pertinent background about DOT's role in protecting consumer privacy and enforcing Privacy Shield.

1. Background

A. DOT's Privacy Authority

The Department is strongly committed to ensuring the privacy of information provided by consumers to airlines and ticket agents. The DOT's authority to take action in this area is found in 49 U.S.C. 41712, which prohibits a carrier or ticket agent from engaging in "an unfair or deceptive practice or an unfair method of competition" in the sale of air transportation that

results or is likely to result in consumer harm. Section 41712 is patterned after Section 5 of the Federal Trade Commission (FTC) Act (15 U.S.C. 45). We interpret our unfair or deceptive practice statute as prohibiting an airline or ticket agent from: (1) violating the terms of its privacy policy; or (2) gathering or disclosing private information in a way that violates public policy, is immoral, or causes substantial consumer injury not offset by any countervailing benefits. We also interpret section 41712 as prohibiting carriers and ticket agents from: (1) violating any rule issued by the Department that identifies specific privacy practices as unfair or deceptive; or (2) violating the Children's Online Privacy Protection Act (COPPA), or FTC rules implementing COPPA. Under Federal law, DOT has exclusive authority to regulate the privacy practices of airlines, and it shares jurisdiction with the FTC with respect to the privacy practices of ticket agents in the sale of air transportation.

As such, once a carrier or seller of air transportation publicly commits to Privacy Shield's privacy principles, the Department is able to use the statutory powers of section 41712 to ensure compliance with those principles. Therefore, once a passenger provides information to a carrier or ticket agent that has committed to honoring Privacy Shield's privacy principles, any failure to do so by the carrier or ticket agent would be a violation of section 41712.

B. Enforcement Practices

The Department's Office of Aviation Enforcement and Proceedings (Aviation Enforcement Office) investigates and prosecutes cases under 49 U.S.C. 41712. It enforces the statutory prohibition in section 41712 against unfair and deceptive practices primarily through negotiation, preparing cease and desist orders, and drafting orders assessing civil penalties. The office learns of potential violations largely from complaints it receives from individuals, travel agents, airlines, and U.S. and foreign government agencies. Consumers may use DOT's website to file privacy complaints against airlines and ticket agents.[1]

If a reasonable and appropriate settlement in a case is not reached, the Aviation Enforcement Office has the authority to institute an enforcement proceeding involving an evidentiary hearing before a DOT administrative law judge (ALJ). The ALJ has the authority to issue cease-and-desist orders and civil penalties. Violations of section 41712 can result in the issuance of cease and desist orders and the imposition of civil penalties of up to $32,140 for each violation of section 41712.

The Department does not have the authority to award damages or provide pecuniary relief to individual complainants. However, the Department does have the authority to approve settlements resulting from investigations brought by its Aviation Enforcement Office that directly benefit consumers (e.g., cash, vouchers) as an offset to monetary penalties otherwise payable to the U.S. Government. This has occurred in the past, and may also occur in the context of Privacy Shield principles when circumstances warrant. Repeated violations of section 41712 by an airline would also raise questions regarding the airline's compliance disposition, which could, in egregious situations, result in an airline being found to be no longer fit to operate and, therefore, losing its economic operating authority.

[1] http://www.transportation.gov/airconsumer/privacy-complaints.

To date, DOT has received relatively few complaints involving alleged privacy violations by ticket agents or airlines. When they arise, they are investigated according to the principles set forth above.

C. DOT Legal Protections Benefiting Swiss Consumers

Under section 41712, the prohibition on unfair or deceptive practices in air transportation or the sale of air transportation applies to U.S. and foreign air carriers as well as ticket agents. The DOT frequently takes action against U.S. and foreign airlines for practices that affect both foreign and U.S. consumers on the basis that the airline's practices took place in the course of providing transportation to or from the United States. The DOT does and will continue to use all remedies that are available to protect both foreign and U.S. consumers from unfair or deceptive practices in air transportation by regulated entities.

The DOT also enforces, with respect to airlines, other targeted laws whose protections extend to non-U.S. consumers such as COPPA. Among other things, COPPA requires that operators of child-directed websites and online services, or general audience sites that knowingly collect personal information from children under 13 provide parental notice and obtain verifiable parental consent. U.S.-based websites and services that are subject to COPPA and collect personal information from foreign children are required to comply with COPPA. Foreign-based websites and online services must also comply with COPPA if they are directed to children in the United States, or if they knowingly collect personal information from children in the United States. To the extent that U.S. or foreign airlines doing business in the United States violate COPPA, DOT would have jurisdiction to take enforcement action.

II. Privacy Shield Enforcement

If an airline or ticket agent chooses to participate in Privacy Shield and the Department receives a complaint that such an airline or ticket agent had allegedly violated Privacy Shield, the Department would take the following steps to vigorously enforce Privacy Shield.

A. Prioritizing Investigation of Alleged Violations

The Department's Aviation Enforcement Office will investigate each complaint alleging Privacy Shield violations (including complaints received from the Federal Data Protection and Information Commissioner and take enforcement action where there is evidence of a violation. Further, the Aviation Enforcement Office will cooperate with the FTC and Department of Commerce and place a priority on allegations that the regulated entities are not complying with privacy commitments made as part of Privacy Shield.

Upon receipt of an allegation of a violation of Privacy Shield, the Department's Aviation Enforcement Office may take a range of actions as part of its investigation. For example, it may review the ticket agent or airline's privacy policies, obtain further information from the ticket agent or airline or from third parties, follow up with the referring entity, and assess whether there is a pattern of violations or significant number of consumers affected. In addition, it would determine whether the issue implicates matters within the purview of the Department of

Commerce or FTC, assess whether consumer education and business education would be helpful, and as appropriate, initiate an enforcement proceeding.

If the Department becomes aware of potential Privacy Shield violations by ticket agents, it will coordinate with the FTC on the matter. We will also advise the FTC and the Department of Commerce of the outcome of any Privacy Shield enforcement action.

B. Addressing False or Deceptive Membership Claims

The Department remains committed to investigating Privacy Shield violations, including false or deceptive claims of membership in Privacy Shield. We will give priority consideration to referrals from the Department of Commerce regarding organizations that it identifies as improperly holding themselves out to be current members of Privacy Shield or using the Privacy Shield certification mark without authorization.

In addition, we note that if an organization's privacy policy promises that it complies with the substantive Privacy Shield principles, its failure to make or maintain a registration with the Department of Commerce likely will not, by itself, excuse the organization from DOT enforcement of those commitments.

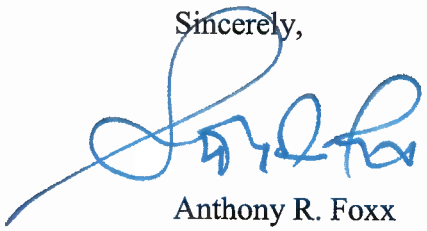
C. Monitoring and Making Public Enforcement Orders Concerning Privacy Shield Violations

The Department's Aviation Enforcement Office also remains committed to monitoring enforcement orders as needed to ensure compliance with Privacy Shield. Specifically, if the office issues an order directing an airline or ticket agent to cease and desist from future violations of Privacy Shield and section 41712, it will monitor the entity's compliance with the cease-and-desist provision in the order. In addition, the office will ensure that orders resulting from Privacy Shield cases are available on its website.

We look forward to our continued work with our Federal partners and Swiss stakeholders on Privacy Shield matters.

I hope that this information proves helpful. If you have any questions or need further information, please feel free to call me.

Sincerely,



Anthony R. Foxx