EUROPEAN
COMMISSION

Brussels, 12.7.2016
C(2016) 4176 final

ANNEXES 1 to 7

ANNEXES

to the

Commission Implementing Decision

pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield

ANNEX I
Letter from U.S. Secretary of Commerce Penny Pritzker

July 7, 2016

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

Dear Commissioner Jourová:

On behalf of the United States, I am pleased to transmit herewith a package of EU-U.S. Privacy Shield materials that is the product of two years of productive discussions among our teams. This package, along with other materials available to the Commission from public sources, provides a very strong basis for a new adequacy finding by the European Commission.[1]

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

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

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

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

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

[1] Provided that the Commission Decision on the adequacy of the protection provided by the EU-U.S. Privacy Shield applies to Iceland, Liechtenstein and Norway, the Privacy Shield Package will cover both the European Union, as well as these three countries.

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

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

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

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

Sincerely,

Penny Pritzker

Annex 1: Letter from Acting Under Secretary for International Trade Ken Hyatt

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

Dear Commissioner Jourová:

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

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

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

Enhancements under the Privacy Shield Principles

The resulting Privacy Shield strengthens the protection of privacy by:

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

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

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

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

Provide Additional Information on the Privacy Shield Website

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

Verify Self-Certification Requirements

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

    - provided required organization contact information;
    - described the activities of the organization with respect to personal information received from the EU;
    - indicated what personal information is covered by its self-certification;
    - if the organization has a public website, provided the web address where the privacy policy is available and the privacy policy is accessible at the web address provided, or if an organization does not have a public website, provided where the privacy policy is available for viewing by the public;
    - included in its relevant privacy policy a statement that it adheres to the Principles and if the privacy policy is available online, a hyperlink to the Department's Privacy Shield website;
    - identified the specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the Principles or a future annex to the Principles);
    - if the organization elects to satisfy the requirements in points (a)(i) and (a)(iii) of the Recourse, Enforcement and Liability Principle by committing to cooperate with the appropriate EU data protection authorities ("DPAs"), indicated its

intention to cooperate with DPAs in the investigation and resolution of complaints brought under the Privacy Shield, notably to respond to their inquiries when EU data subjects have brought their complaints directly to their national DPAs;
    - identified any privacy program in which the organization is a member;
    - identified the method of verification of assuring compliance with the Principles (*e.g.*, in-house, third party);
    - identified, both in its self-certification submission and in its privacy policy, the independent recourse mechanism that is available to investigate and resolve complaints;
    - included in its relevant privacy policy, if the policy is available online, a hyperlink to the website or complaint submission form of the independent recourse mechanism that is available to investigate unresolved complaints; and
    - if the organization has indicated that it intends to receive human resources information transferred from the EU for use in the context of the employment relationship, declared its commitment to cooperate and comply with DPAs to resolve complaints concerning its activities with regard to such data, provided the Department with a copy of its human resources privacy policy, and provided where the privacy policy is available for viewing by its affected employees.

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

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

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

Search for and Address False Claims of Participation

- review the privacy policies of organizations that have previously participated in the Privacy Shield program, but that have been removed from the Privacy Shield List to identify any false claims of Privacy Shield participation;
- on an ongoing basis, when an organization: (a) withdraws from participation in the Privacy Shield, (b) fails to recertify its adherence to the Principles, or (c) is removed as a participant in the Privacy Shield notably for "persistent failure to comply," undertake, on an *ex officio* basis, to verify that the organization has removed from any relevant published privacy policy any references to the Privacy Shield that imply that the organization continues to actively participate in the Privacy Shield and is entitled to its benefits. Where the Department finds that such references have not been removed, the Department will warn the organization that the Department will, as appropriate, refer

matters to the relevant agency for potential enforcement action if it continues to make the claim of Privacy Shield certification. If the organization neither removes the references nor self-certifies its compliance under the Privacy Shield, the Department will *ex officio* refer the matter to the FTC, DOT, or other appropriate enforcement agency or, in appropriate cases, take action to enforce the Privacy Shield certification mark;

- undertake other efforts to identify false claims of Privacy Shield participation and improper use of the Privacy Shield certification mark, including by conducting Internet searches to identify where images of the Privacy Shield certification mark are being displayed and references to Privacy Shield in organizations' privacy policies;
- promptly address any issues that we identify during our *ex officio* monitoring of false claims of participation and misuse of the certification mark, including warning organizations misrepresenting their participation in the Privacy Shield program as described above;
- take other appropriate corrective action, including pursuing any legal recourse the Department is authorized to take and referring matters to the FTC, DOT, or another appropriate enforcement agency; and
- promptly review and address complaints about false claims of participation that we receive.

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

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

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

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

Tailor the Privacy Shield Website to Targeted Audiences

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

Increase Cooperation with DPAs

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

regarding the Privacy Shield and the rights and responsibilities it creates should facilitate the identification of issues as they arise, so that these can be appropriately addressed.

Facilitate Resolution of Complaints about Non-Compliance

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

Adopt Arbitral Procedures and Select Arbitrators in Consultation with the Commission

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

Joint Review Mechanism of the Functioning of the Privacy Shield

The Department of Commerce, the FTC, and other agencies, as appropriate, will hold annual meetings with the Commission, interested DPAs, and appropriate representatives from the Article 29 Working Party, where the Department will provide updates on the Privacy Shield program. The annual meetings will include discussion of current issues related to the functioning, implementation, supervision, and enforcement of the Privacy Shield, including referrals received by the Department from DPAs, the results of *ex officio* compliance reviews, and may also include discussion of relevant changes of law. The first annual review and subsequent reviews as appropriate will include a dialogue on other topics, such as in the area of automated decision-making, including aspects relating to similarities and differences in approaches in the EU and the US.

Update of Laws

The Department will make reasonable efforts to inform the Commission 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 thesehave been forwarded to you. 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 Commission is 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 Commission will determine that the EU-U.S. Privacy Shield Framework provides adequate protection for the purposes of EU law and data transfers from the European Union will continue to organizations that participate in the Privacy Shield.

Sincerely,

Ken Hyatt

Annex 2: Arbitral Model

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 EU-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.

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[1] 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 their Data Protection Authority 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.

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 an EU Data Protection

[1] Section I.5 of the Principles.

Authority (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. A DPA's authority to resolve the same claim against an EU data controller does not alone preclude invocation of this arbitration option against a different legal entity not bound by the DPA 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.[2] 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 EU or U.S. courts, or FTC proceedings.

F. The Arbitration Panel

[2] 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.

The parties will select the arbitrators from the list of arbitrators discussed below.

Consistent with applicable law, the U.S. Department of Commerce and the European Commission will develop a list of at least 20 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., 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 EU data protection law.

G. Arbitration Procedures

Consistent with applicable law, within 6 months from the adoption of the adequacy decision, the Department of Commerce and the European Commission will agree to adopt an existing, well-established set of U.S. arbitral procedures (such as AAA or JAMS) to govern proceedings before the Privacy Shield Panel, subject to each of the following considerations:

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. No representative of the U.S., EU, 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 an EU individual, EU DPAs may provide assistance in the preparation only of the Notice but EU DPAs may not have access to discovery or any other materials related to these arbitrations.
5. 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.
6. 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.
7. Materials submitted to arbitrators will be treated confidentially and will only be used in connection with the arbitration.
8. 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.

9. 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.

H. Costs

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

Subject to applicable law, the Department of Commerce will facilitate the establishment of a fund, 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 European Commission. The fund will be managed by a third party, which will report regularly on the operations of the fund. At the annual review, the Department of Commerce and European Commission 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.

ANNEX II

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

I. OVERVIEW

1. While the United States and the European Union share the goal of enhancing privacy protection, the United States takes a different approach to privacy from that taken by the European Union. 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 the European Union while ensuring that EU data subjects continue to benefit from effective safeguards and protection as required by European legislation with respect to the processing of their personal data when they have been transferred to non-EU 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). The Principles were developed in consultation with the European Commission, and with industry and other stakeholders, to facilitate trade and commerce between the United States and European Union. They are intended for use solely by organizations in the United States receiving personal data from the European Union for the purpose of qualifying for the Privacy Shield and thus benefitting from the European Commission's adequacy decision.[1] The Principles do not affect the application of national provisions implementing Directive 95/46/EC ("the Directive") that apply to the processing of personal data in the Member States. 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 the EU, 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 the EU 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

[1] Provided that the Commission Decision on the adequacy of the protection provided by the EU-U.S. Privacy Shield applies to Iceland, Liechtenstein and Norway, the Privacy Shield Package will cover both the European Union, as well as these three countries. Consequently, references to the EU and its Member States will be read as including Iceland, Liechtenstein and Norway.

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 the European Commission's adequacy decision to receive personal information from the EU. 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 the European Commission's adequacy decision that would enable those organizations to receive personal information from the EU. 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 the Directive or Member State law 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 the EU 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 European data protection authorities ("DPAs"). 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 Directive, received by an organization in the United States from the European Union, 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 the European Commission's adequacy determination.

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 the EU 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 the EU 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 panel established by DPAs, (2) an alternative dispute resolution provider based in the EU, 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, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), 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.[2] An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or 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,

[2] 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.

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[3] 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;

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

[3] 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."

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 EU Member State authorities through the Department. Organizations that have chosen to cooperate with DPAs, 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 DPAs 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 EU Member State authorities, and will exchange information regarding referrals with the referring state authorities 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 Directive's 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 Directive 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 Data Protection Authorities

a. Organizations will implement their commitment to cooperate with European Union data protection authorities ("DPAs"**)** as described below. Under the Privacy Shield, U.S. organizations receiving personal data from the EU 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 DPAs.

b. An organization commits to cooperate with the DPAs 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 DPAs;

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

iii. will comply with any advice given by the DPAs where the DPAs take 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 DPAs with written confirmation that such action has been taken.

c. Operation of DPA Panels

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

1. The advice of the DPAs will be delivered through an informal panel of DPAs established at the European Union level, which will *inter alia* help ensure a harmonized and coherent approach.

2. The panel 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 the EU 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 DPAs consider appropriate.

3. The panel 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 DPAs 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 panel will seek to deliver advice as quickly as this requirement for due process allows. As a general rule, the panel will aim to provide advice within 60 days after receiving a complaint or referral and more quickly where possible.

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

6. The delivery of advice through the panel will not give rise to any liability for the panel or for individual DPAs.

ii. As noted above, organizations choosing this option for dispute resolution must undertake to comply with the advice of the DPAs. 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 panel 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 panel 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 DPAs, 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 the EU in the context of the employment relationship must commit to cooperate with the DPAs with regard to such data (*see* Supplemental Principle on Human Resources Data).

e. Organizations choosing this option will be required to pay an annual fee which will be designed to cover the operating costs of the panel, and they may additionally be asked to meet any necessary translation expenses arising out of the panel's consideration of referrals or complaints against them. The annual fee will not exceed USD 500 and will be less for smaller companies.

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 the EU; 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 the EU 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 EU authority or authorities concerned in conformity with the Supplemental Principles on Human Resources Data and the Role of the Data Protection Authorities as applicable and that it will comply with the advice given by such authorities. 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. Recognizing that the Principles will impact commercial relationships with third parties, organizations that certify to the Privacy Shield Framework in the first two months following the Framework's effective date shall bring existing commercial relationships with third parties into conformity with the Accountability for Onward Transfer Principle as soon as possible, and in any event no later than nine months from the date upon which they certify to the Privacy Shield. During that interim period, where organizations transfer data to a third party, they shall (i) apply the Notice and Choice Principles, and (ii) where personal data is transferred to a third party acting as an agent, ascertain that the agent is obligated to provide at least the same level of protection as is required by the Principles.

f. An organization must subject to the Privacy Shield Principles all personal data received from the EU 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 European Commission); 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 EU-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 the EU 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 the EU 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. <u>The Access Principle in Practice</u>

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;[4]

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

[4] 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.

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.

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 Directive, 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 the EU 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 the EU country where it was collected, 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 the EU 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 authorised by the individual. Moreover, such choices must not be used to restrict employment opportunities or take any punitive action against such employees.

ii. It should be noted that certain generally applicable conditions for transfer from some EU Member States may preclude other uses of such information even after transfer outside the EU and such conditions will have to be respected.

iii. 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.

iv. 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 the European Union must comply with local regulations and ensure that European Union employees have access to such information as is required by law in their home countries, 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 EU 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 the EU. It follows that, where European 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 state or national data protection 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 EU human resources data transferred from the European Union 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 competent EU authorities 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 the EU 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 the European Union are always required to enter into a contract when a transfer for mere processing is

made, whether the processing operation is carried out inside or outside the EU, 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, alternation, 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 EU Member States), 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 EU 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 data protection authorities located in the European Union or their authorized representatives.

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 DPAs. 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[5] or with respect to an allegation about the adequacy of the Privacy Shield. Under this arbitration option, the Privacy Shield Panel

[5] Section I.5 of the Principles.

(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. 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.[6] 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) EU Member States; 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

[6] 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.

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 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 the EU in several different circumstances. Under Article 26 of the Directive, personal data may be transferred "to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2)" on the condition that it (i) 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) has been unambiguously consented to by the consumer. U.S. organizations subscribing to the Privacy Shield provide adequate protection for personal data and may therefore receive data transfers from the EU without meeting these conditions or other conditions set out in Article 26 of the Directive. 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 the EU Member State in which it is operating, which may inter alia impose special conditions for the handling of sensitive data.

14. Pharmaceutical and Medical Products

a. Application of EU Member State Laws or the Privacy Shield Principles

i. EU Member State 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 the EU 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 the EU 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 European 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: ARBITRAL MODEL

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 EU-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.

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[7] 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 their Data Protection Authority 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.

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 an EU Data Protection

Authority (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. A DPA's authority

[7] Section I.5 of the Principles.

to resolve the same claim against an EU data controller does not alone preclude invocation of this arbitration option against a different legal entity not bound by the DPA 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.[8] 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 EU or U.S. courts, or FTC proceedings.

F. The Arbitration Panel

The parties will select the arbitrators from the list of arbitrators discussed below.

---

[8]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.

Consistent with applicable law, the U.S. Department of Commerce and the European Commission will develop a list of at least 20 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., 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 EU data protection law.

G. Arbitration Procedures

Consistent with applicable law, within 6 months from the adoption of the adequacy decision, the Department of Commerce and the European Commission will agree to adopt an existing, well-established set of U.S. arbitral procedures (such as AAA or JAMS) to govern proceedings before the Privacy Shield Panel, subject to each of the following considerations:

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. No representative of the U.S., EU, 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 an EU individual, EU DPAs may provide assistance in the preparation only of the Notice but EU DPAs may not have access to discovery or any other materials related to these arbitrations.
5. 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.

6. 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.
7. Materials submitted to arbitrators will be treated confidentially and will only be used in connection with the arbitration.
8. 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.
9. 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.

H. Costs

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

Subject to applicable law, the Department of Commerce will facilitate the establishment of a fund, 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 European Commission. The fund will be managed by a third party, which will report regularly on the operations of the fund. At the annual review, the Department of Commerce and European Commission 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.

ANNEX III
Letter from U.S. Secretary of State John Kerry

July 7, 2016

Dear Commissioner Jourová,

I am pleased we have reached an understanding on the European Union-United States Privacy Shield that will include an Ombudsperson mechanism through which authorities in the EU will be able to submit requests on behalf of EU 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, I designated Under Secretary of State Catherine A. Novelli, who also serves as Senior Coordinator for International Information Technology Diplomacy, as our point of contact for foreign governments that wish to raise concerns regarding U.S. signals intelligence activities. Building on this role, I have established a Privacy Shield Ombudsperson mechanism in accordance with the terms set out in Annex A**,** which have been updated since my letter of February 22, 2016. I have directed Under Secretary Novelli to perform this function. Under Secretary Novelli is independent from the U.S. intelligence community, and reports directly to me.

I have directed my staff to devote the necessary resources to implement this new Ombudsperson mechanism, and am confident it will be an effective means to address EU individuals' concerns.

Sincerely,

John F. Kerry

ANNEX A

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

In recognition of the importance of the EU-U.S. Privacy Shield Framework, this Memorandum sets forth the process for implementing a new mechanism, consistent with Presidential Policy Directive 28 (PPD-28), regarding signals intelligence.[1]

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 new mechanism that the Senior Coordinator will follow to facilitate the processing of requests relating to national security access to data transmitted from the EU to the United States pursuant to the Privacy Shield, standard contractual clauses (SCCs), binding corporate rules (BCRs), "Derogations,"[2] or "Possible Future Derogations,"[3] through

[1] Provided that the Commission Decision on the adequacy of the protection provided by the EU-U.S. Privacy Shield applies to Iceland, Liechtenstein and Norway, the Privacy Shield Package will cover both the European Union, as well as these three countries. Consequently, references to the EU and its Member States will be read as including Iceland, Liechtenstein and Norway.

[2] "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.

[3] "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 the EU 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

established avenues under applicable United States laws and policy, and the response to those requests.

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 from the submitting EU individual complaint handing body 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. A request will initially be submitted to the supervisory authorities in the Member States competent for the oversight of national security services and/or the processing of personal data by public authorities. The request will be submitted to the Ombudsperson

---

surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data.

by a EU centralized body (hereafter together: the "EU individual complaint handling body").

b. The EU individual complaint handling body will ensure, in compliance with the following actions, that the request is complete:

(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 the EU 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 Submitting EU Individual Complaint Handling Body**.

a. The Privacy Shield Ombudsperson will acknowledge receipt of the request to the submitting EU individual complaint handling body.

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 submitting EU individual complaint handling body.

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 submitting EU individual complaint handling body.

d. The Privacy Shield Ombudsperson will track the status of requests and provide updates as appropriate to the submitting EU individual complaint handling body.

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 submitting EU individual complaint handling body, subject to the continuing obligation to protect information under applicable laws and policies. The Privacy Shield Ombudsperson will provide a response to the submitting EU individual complaint handling body 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 EU individual complaint handling body, 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 EU-U.S. Privacy Shield is inconsistent with European Union data protection requirements. The commitments in this Memorandum are made based on the common understanding by the European Commission 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 European Commission any adjustments that may be appropriate to address the situation.

5. **Requests for Information.** Requests for access to United States 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 each EU Member State with its own information access law. 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 United States 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.

ANNEX IV
Letter from Federal Trade Commission Chairwoman Edith Ramirez

July 7, 2016

VIA EMAIL

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

Dear Commissioner Jourová:

The United States Federal Trade Commission ("FTC") appreciates the opportunity to describe its enforcement of the new EU-U.S. Privacy Shield Framework (the "Privacy Shield Framework" or "Framework"). We believe the Framework will play a critical role in facilitating privacy-protective commercial transactions in an increasingly interconnected world. It will enable businesses to conduct important operations in the global economy, while at the same time ensuring that EU consumers retain important privacy protections. The FTC has long committed to protecting privacy across borders and will make enforcement of the new Framework a high priority. Below, we explain the FTC's history of strong privacy enforcement generally, including our enforcement of the original Safe Harbor program, as well as the FTC's approach to enforcement of the new Framework.

The FTC first publicly expressed its commitment to enforce the Safe Harbor program in 2000. At that time, then-FTC Chairman Robert Pitofsky sent the European Commission a letter outlining the FTC's pledge to vigorously enforce the Safe Harbor Privacy Principles. The FTC has continued to uphold this commitment through nearly 40 enforcement actions, numerous additional investigations, and cooperation with individual European data protection authorities ("EU DPAs") on matters of mutual interest.

After the European Commission raised concerns in November 2013 about the administration and enforcement of the Safe Harbor program, we and the U.S. Department of Commerce began consultations with officials from the European Commission to explore ways to strengthen it. While those consultations were proceeding, on October 6, 2015, the European Court of Justice issued a decision in the *Schrems* case that, among other things, invalidated the European Commission's decision on the adequacy of the Safe Harbor program. Following the decision, we continued to work closely with the Department of Commerce and the European Commission in an effort to strengthen the privacy protections provided to EU individuals. The Privacy Shield Framework is a result of these ongoing consultations. As was the case with the Safe Harbor program, the FTC hereby commits to vigorous enforcement of the new Framework. This letter memorializes that commitment.

Notably, we affirm our 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 with EU DPAs. We provide below detailed information about each of these commitments and relevant background about the FTC's role in protecting consumer privacy and enforcing Safe Harbor, as well as the broader privacy landscape in the United States.[1]

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.[2] A representation, omission, or practice is deceptive if it is material and likely to mislead consumers acting reasonably under the circumstances.[3] 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.[4] 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. 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.[5] 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

[1] We provide additional information about U.S. federal and state privacy laws 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.
[2] 15 U.S.C. § 45(a).
[3] 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.
[4] 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.
[5] See California Dental Ass'n v. FTC, 526 U.S. 756 (1999).

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

The FTC has also pursued numerous policy initiatives aimed at enhancing consumer privacy that inform its enforcement work. 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.

The FTC also engages in consumer and business education to enhance the impact of its enforcement and policy development initiatives. The FTC has used a variety of tools—publications, online resources, workshops, and social media—to provide educational materials on a wide range of topics, including mobile apps, children's privacy, and data security. Most recently, the Commission launched its "Start With Security" initiative, which includes new guidance for businesses drawing on lessons learned from the agency's data security cases, as well as a series of workshops across the country. In addition, the FTC has long been a leader in educating consumers about basic computer security. Last year, our OnGuard Online site and its Spanish language counterpart, Alerta en Línea, had more than 5 million page views.

B. U.S. Legal Protections Benefiting EU Consumers

The Framework will operate in the context of the larger U.S. privacy landscape, which protects EU consumers in a number of ways.

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.

Indeed, the FTC's enforcement work significantly benefits both U.S. and foreign consumers. For example, our cases enforcing Section 5 of the FTC Act have protected the privacy of U.S. and foreign consumers alike. 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.[6] The court granted injunctive relief against Accusearch prohibiting, among

[6] *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.

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.[7]

The FTC's settlement with TRUSTe is another example. It ensures that consumers, including those in the European Union, can rely on representations that a global self-regulatory organization makes about its review and certification of domestic and foreign online services.[8] Importantly, our action against TRUSTe also strengthens the privacy self-regulatory system more broadly by ensuring the accountability of entities that play an important role in self- regulatory schemes, including cross-border privacy frameworks.

The FTC also enforces other targeted laws whose protections extend to non-U.S. consumers, such as the Children's Online Privacy Protection Act ("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 the age of 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. In addition to the U.S. federal laws enforced by the FTC, certain other federal and state consumer protection and privacy laws may provide additional benefits to EU consumers.

C. Safe Harbor Enforcement

As part of its privacy and security enforcement program, the FTC has also sought to protect 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.[9] 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 Privacy Shield Framework. The FTC can

[7] See *FTC v. Accusearch, Inc.*, No. 06CV015D (D. Wyo. Dec. 20, 2007), *aff'd* 570 F.3d 1187 (10th Cir. 2009).
[8] See *In the Matter of True Ultimate Standards Everywhere, Inc.*, No. C-4512 (F.T.C. Mar. 12, 2015) (decision and order), *available at* https://www ftc.gov/system/files/documents/cases/150318trust-edo.pdf.
[9] 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.

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.

The FTC's cases have also focused on false, deceptive, or misleading claims of Safe Harbor participation. The FTC takes these claims seriously. For example, in *FTC v. Karnani*, the FTC brought an action in 2011 against an Internet marketer in the United States alleging that he and his company tricked British consumers into believing that the company was based in the United Kingdom, including by using .uk web extensions and referencing British currency and the UK postal system.[10] However, when consumers received the products, they discovered unexpected import duties, warranties that were not valid in the United Kingdom, and charges associated with obtaining refunds. The FTC also charged that the defendants deceived consumers about their participation in the Safe Harbor program. Notably, all of the consumer victims were in the United Kingdom.

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 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.[11]

II. Referral Prioritization and Investigations

As we did under the Safe Harbor program, the FTC commits to give priority to Privacy Shield referrals from EU Member States. 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 EU Member States, the FTC is creating a standardized referral process and providing guidance to EU Member States 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 EU Member State 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 an EU Member State or 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

[10] See *FTC v. Karnani*, No. 2:09-cv-05276 (C.D. Cal. May 20, 2011) (stipulated final order), *available at* https://www ftc.gov/sites/default/files/documents/cases/2011/06/110609karnanistip.pdf; *see also* Lesley Fair, FTC Business Center Blog, *Around the World in Shady Ways*, http://www.business.ftc.gov/blog/2011/06/around-world-shady-ways (June 9, 2011).

[11] Letter from Ken Hyatt, Acting Under Secretary of Commerce for International Trade, International Trade Administration, to Věra Jourová, Commissioner for Justice, Consumers and Gender Equality .

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 referring enforcement authorities, 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 referring authority on the types of referrals received in order to increase the effectiveness of efforts to address unlawful conduct. If a referring enforcement authority 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 EU DPAs 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 similar to those prohibited by laws the FTC enforces.[12] As part of this assistance, the FTC can share information obtained in connection with an FTC investigation, issue compulsory process on behalf of the EU 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.[13]

In addition to prioritizing Privacy Shield referrals from EU Member States and privacy self-regulatory organizations,[14] 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

---

[12] 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.

[13] 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.

[14] Although the FTC does not resolve or mediate individual consumer complaints, the FTC affirms that it will prioritize Privacy Shield referrals from EU DPAs. 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. EU individuals can use the same complaint system available to U.S. citizens to submit a complaint to the FTC at www ftc.gov/complaint. For individual Privacy Shield complaints, however, it may be most useful for EU individuals to submit complaints to their Member State DPA or alternative dispute resolution provider.

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 Safe Harbor program 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.

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 $16,000 per violation, or $16,000 per day for a continuing violation,[15] 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.

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.[16] 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 EU DPAs and Enforcement Cooperation

The FTC recognizes the important role that EU DPAs play with respect to Framework compliance and encourages increased consultation and enforcement cooperation. In addition to any consultation with referring DPAs on case-specific matters, the FTC commits to participate in periodic meetings with designated representatives of the Article 29 Working Party to discuss in general terms how to improve enforcement cooperation with respect to the Framework. The FTC will also participate, along with the Department of Commerce, the European Commission, and Article 29 Working Party representatives, 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 EU DPAs, 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 EU DPAs 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 EU 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.

***

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

[16] *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 FTC is pleased to affirm its commitment to enforcing the new Privacy Shield Framework. We also look forward to continuing engagement with our EU colleagues as we work together to protect consumer privacy on both sides of the Atlantic.

Sincerely,

Edith Ramirez
Chairwoman

ATTACHMENT A

The EU-U.S. Privacy Shield Framework in Context: An Overview of the U.S. Privacy and Security Landscape

The protections provided by the EU-U.S. Privacy Shield Framework (the "Framework") exist in the context of the broader privacy protections afforded under the U.S. legal system as a whole. First, the U.S. Federal Trade Commission ("FTC") has a robust privacy and data security program for U.S. commercial practices that protects consumers worldwide. Second, the landscape of consumer privacy and security protection in the United States has evolved substantially since 2000 when the original U.S.-EU Safe Harbor program was adopted. Since that time, many federal and state privacy and security laws have been enacted, and public and private litigation to enforce privacy rights has increased significantly. The broad scope of U.S. legal protections for consumer privacy and security applicable to commercial data practices complements the protections provided to EU individuals by the new Framework.

I. The FTC's General Privacy and Security Enforcement Program

The FTC is the leading U.S. consumer protection agency focused on commercial sector privacy. The FTC has authority to prosecute unfair and deceptive acts or practices that violate consumer privacy, as well as to enforce more targeted privacy laws that protect certain financial and health information, information about children, and information used to make certain eligibility decisions about consumers.

The FTC has unparalleled experience in consumer privacy enforcement. The FTC's enforcement actions have addressed unlawful practices in offline and online environments. For example, the FTC has brought enforcement actions against well-known companies, such as Google, Facebook, Twitter, Microsoft, Wyndham, Oracle, HTC, and Snapchat, as well as lesser- known companies. The FTC has sued businesses that allegedly spammed consumers, installed spyware on computers, failed to secure consumers' personal information, deceptively tracked consumers online, violated children's privacy, unlawfully collected information on consumers' mobile devices, and failed to secure Internet-connected devices used to store personal information. The resulting orders have typically provided for ongoing monitoring by the FTC for a period of twenty years, prohibited further law violations, and subjected the businesses to substantial financial penalties for order violations.[1] Importantly, FTC orders do not just protect the individuals who may have complained about a problem; rather, they protect all consumers dealing with the business going forward. In the cross-border context, the FTC has jurisdiction to protect consumers worldwide from practices taking place in the United States.[2]

[1] Any entity that fails to comply with an FTC order is subject to a civil penalty of up to $16,000 per violation, or $16,000 per day for a continuing violation. *See* 15 U.S.C. § 45(l); 16 C.F.R. § 1.98(c).

[2] Congress has expressly affirmed the FTC's authority to seek legal remedies, including restitution, for any acts or practices involving foreign commerce that (1) cause or are likely to cause reasonably foreseeable injury in the United States, or (2) involve material conduct occurring within the United States. *See* 15 U.S.C. § 45(a)(4).

To date, the FTC has brought over 130 spam and spyware cases, over 120 "Do Not Call" telemarketing cases, over 100 Fair Credit Reporting Act actions, almost 60 data security cases, more than 50 general privacy actions, almost 30 cases for violations of the Gramm-Leach-Bliley Act, and over 20 actions enforcing the Children's Online Privacy Protection Act ("COPPA").[3] In addition to these cases, the FTC has also issued and publicized warning letters.[4]

As part of its history of strong privacy enforcement, the FTC has also regularly looked for potential violations of the Safe Harbor program. Since the Safe Harbor program was adopted, the FTC has undertaken numerous investigations into Safe Harbor compliance on its own initiative and has brought 39 cases against U.S. companies for Safe Harbor violations. The FTC will continue this proactive approach by making enforcement of the new Framework a priority.

II. Federal and State Protections for Consumer Privacy

The Safe Harbor Enforcement Overview, which appears as an annex to the European Commission's Safe Harbor adequacy decision, provides a summary of many of the federal and state privacy laws in place at the time the Safe Harbor program was adopted in 2000.[5] At that time, many federal statutes regulated the commercial collection and use of personal information, beyond Section 5 of the FTC Act, including: the Cable Communications Policy Act, the Driver's Privacy Protection Act, the Electronic Communications Privacy Act, the Electronic Funds Transfer Act, the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, the Right to Financial Privacy Act, the Telephone Consumer Protection Act, and the Video Privacy Protection Act. Many states had analogous laws in these areas as well.

Since 2000, there have been numerous developments at both the federal and state level that provide additional consumer privacy protections.[6] At the federal level, for example, the FTC amended the COPPA Rule in 2013 to provide a number of additional protections for children's personal information. The FTC also issued two rules implementing the Gramm- Leach-Bliley Act – the Privacy Rule and the Safeguards Rule – which require financial institutions[7] to make disclosures about their information sharing

---

[3] In some instances, the Commission's privacy and data security cases allege that a company engaged in both deceptive and unfair practices; these cases also sometimes involve alleged violations of multiple statutes, such as the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, and COPPA.

[4] *See, e.g.*, Press Release, Fed. Trade Comm'n, FTC Warns Children's App Maker BabyBus About Potential COPPA Violations (Dec. 22, 2014), https://www.ftc.gov/news-events/press- releases/2014/12/ftc-warns-childrens-app-maker-babybus-about-potential-coppa; Press Release, Fed. Trade Comm'n, FTC Warns Data Broker Operations of Possible Privacy Violations (May 7, 2013), https://www.ftc.gov/news-events/press-releases/2013/05/ftc-warns-data-broker-operations-possible- privacy-violations; Press Release, Fed. Trade Comm'n, FTC Warns Data Brokers That Provide Tenant Rental Histories They May Be Subject to Fair Credit Reporting Act (Apr. 3, 2013), https://www.ftc.gov/news-events/press-releases/2013/04/ftc-warns-data-brokers-provide-tenant-rental- histories-they-may.

[5] *See* U.S. Dep't of Commerce, Safe Harbor Enforcement Overview, https://build.export.gov/main/safeharbor/eu/eg_main_018481.

[6] For a more comprehensive summary of the legal protections in the United States, see Daniel J. Solove & Paul Schwartz, *Information Privacy Law* (5th ed. 2015).

[7] Financial institutions are defined very broadly under the Gramm-Leach-Bliley Act to include all businesses that are "significantly engaged" in providing financial products or services. This includes, for example, check-cashing businesses, payday lenders, mortgage brokers, nonbank lenders, personal property or real estate appraisers, and professional tax preparers.

practices and to implement a comprehensive information security program to protect consumer information.[8] Similarly, the Fair and Accurate Credit Transactions Act ("FACTA"), enacted in 2003, supplements longstanding U.S. credit laws to establish requirements for the masking, sharing, and disposal of certain sensitive financial data. The FTC promulgated a number of rules under FACTA regarding, among other things, consumers' right to a free annual credit report; secure disposal requirements for consumer report information; consumers' right to opt out of receiving certain offers of credit and insurance; consumers' right to opt out of the use of information provided by an affiliated company to market its products and services; and requirements for financial institutions and creditors to implement identity theft detection and prevention programs.[9] In addition, rules promulgated under the Health Insurance Portability and Accountability Act were revised in 2013, adding additional safeguards to protect the privacy and security of personal health information.[10] Rules protecting consumers from unwanted telemarketing calls, robocalls, and spam have also gone into effect. Congress has also enacted laws requiring certain companies that collect health information to provide consumers with notification in the event of a breach.[11]

States have also been very active in passing laws related to privacy and security. Since 2000, forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted laws requiring businesses to notify individuals of security breaches of personal information.[12] At least thirty-two states and Puerto Rico have data disposal laws, establishing requirements for the destruction or disposal of personal information.[13] A number of states also have enacted general data security laws. In addition, California has enacted various privacy laws, including a law requiring companies to have privacy policies and disclose their Do Not Track practices,[14] a "Shine the Light" law requiring greater transparency for data brokers,[15] and a law that mandates an "eraser button" allowing minors to request the deletion of certain social media information.[16] Using these laws and other authorities, federal and state governments have levied significant fines against companies that have failed to protect the privacy and security of consumers' personal information.[17]

---

[8] Under the Consumer Financial Protection Act of 2010 ("CFPA"), Title X of Pub. L. 111-203, 124 Stat. 1955 (July 21, 2010) (also known as the "Dodd-Frank Wall Street Reform and Consumer Protection Act"), most of the FTC's Gramm-Leach-Bliley Act rulemaking authority was transferred to the Consumer Financial Protection Bureau ("CFPB"). The FTC retains enforcement authority under the Gramm-Leach- Bliley Act as well as rulemaking authority for the Safeguards Rule and limited rulemaking authority under the Privacy Rule with respect to auto dealers.

[9] Under the CFPA, the Commission shares its FCRA enforcement role with the CFPB, but rulemaking authority transferred in large part to the CFPB (with the exception of the Red Flags and Disposal Rules).

[10] *See* 45 C.F.R. pts. 160, 162, 164.

[11] *See, e.g.*, American Recovery & Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009) and relevant regulations, 45 C.F.R. §§ 164.404-164.414; 16 C.F.R. pt. 318.

[12] *See, e.g.*, National Conference of State Legislatures ("NCSL"), *State Security Breach Notification Laws* (Jan. 4, 2016), *available at* http://www.ncsl.org/research/telecommunications-and-information- technology/security-breach-notification-laws.aspx.

[13] NCSL, *Data Disposal Laws* (Jan. 12, 2016), *available at* http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

[14] Cal. Bus. & Professional Code §§ 22575-22579.

[15] Cal. Civ. Code §§ 1798.80-1798.84.

[16] Cal. Bus. & Professional Code § 22580-22582.

[17] *See* Jay Cline, *U.S. Takes the Gold in Doling Out Privacy Fines*, Computerworld (Feb. 17, 2014), *available at*

Private lawsuits have also led to successful judgments and settlements that provide additional privacy and data security protection for consumers. For example, in 2015, Target agreed to pay $10 million as part of a settlement with customers who claimed their personal financial information was compromised by a widespread data breach. In 2013, AOL agreed to pay a $5 million settlement to resolve a class action involving alleged inadequate de-identification related to the release of search queries of hundreds of thousands of AOL members. Additionally, a federal court approved a $9 million payment by Netflix for allegedly keeping rental history records in violation of the Video Privacy Protection Act of 1988. Federal courts in California approved two separate settlements with Facebook, one for $20 million and another for $9.5 million, involving the company's collection, use, and sharing of its users' personal information. And, in 2008, a California state court approved a $20 million settlement with LensCrafters for unlawful disclosure of consumers' medical information.

In sum, as this summary illustrates, the United States provides significant legal protection for consumer privacy and security. The new Privacy Shield Framework, which ensures meaningful safeguards for EU individuals, will operate against this larger backdrop in which the protection of consumers' privacy and security continues to be an important priority.

---

http://www.computerworld.com/s/article/9246393/Jay_Cline_U.S._takes_the_gold_in_doling_out_privac y fines?taxonomyId=17&pageNumber=1.

ANNEX V:
Letter from U.S. Secretary of Transportation Anthony Foxx

February 19, 2016

Commissioner Vera Jourová
European Commission
Rue de la Loi / Wetstraat 200
1049 1049 Brussels
Belgium

Re: EU-U.S. Privacy Shield Framework

Dear Commissioner Jourová:

The United States Department of Transportation ("Department" or "DOT") appreciates the opportunity to describe its role in enforcing the EU-U.S. Privacy Shield Framework. This Framework 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 EU consumers retain important privacy protections.

The DOT first publicly expressed its commitment to enforcement of the Safe Harbor Framework in a letter sent to the European Commission over 15 years ago. 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, the 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 the DOT's role in protecting consumer privacy and enforcing the Privacy Shield Framework.

I. 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 act ion 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, the 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 the Privacy Shield Framework'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 the Privacy Shield Framework'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 the 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 $27,500 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 the Privacy Shield Framework

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

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.

To date, the 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 EU 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, the DOT would have jurisdiction to take enforcement action.

II. Privacy Shield Enforcement

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

A. Prioritizing Investigation of Alleged Violations

The Department's Aviation Enforcement Office will investigate each complaint alleging Privacy Shield violations (including complaints received from EU Data Protection Authorities) 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 give priority consideration to allegations that the regulated entities are not complying with privacy commitments made as part of the Privacy Shield Framework.

Upon receipt of an allegation of a violation of the Privacy Shield Framework, 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 the Privacy Shield Program. 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 Framework 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 the Privacy Shield program. 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 EU 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 contact me.

Sincerely

Anthony R. Foxx
Secretary of Transportation

ANNEX VI

Letter from General Counsel Robert Litt
Office of the Director of National Intelligence

February 22, 2016

Mr. Justin S. Antonipillai
Counselor
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, DC 20230

Mr. Ted Dean
Deputy Assistant Secretary
International Trade Administration
1401 Constitution Ave., NW
Washington, DC 20230

Dear Mr. Antonipillai and Mr. Dean:

Over the last two and a half years, in the context of negotiations for the EU-U.S. Privacy Shield, the United States has provided substantial information about the operation of U.S. Intelligence Community signals intelligence collection activity. This has included information about the governing legal framework, the multi-layered oversight of those activities, the extensive transparency about those activities, and the overall protections for privacy and civil liberties, in order to assist the European Commission in making a determination about the adequacy of those protections as they relate to the national security exception to the Privacy Shield principles. This document summarizes the information that has been provided.

I. PPD-28 and the Conduct of U.S. Signals Intelligence Activity

The U.S. Intelligence Community collects foreign intelligence in a carefully controlled manner, in strict accordance with U.S. laws and subject to multiple layers of oversight, focusing on important foreign intelligence and national security priorities. A mosaic of laws and policies governs U.S. signals intelligence collection, including the U.S. Constitution, the Foreign Intelligence Surveillance Act (50 U.S.C. § 1801 *et seq.*) (FISA), Executive Order 12333 and its implementing procedures, Presidential guidance, and numerous procedures and guidelines, approved by the FISA Court and the Attorney General, that establish additional rules limiting the collection, retention, use, and dissemination of foreign intelligence information.[1]

a. PPD 28 Overview

[1] Further information concerning U.S. foreign intelligence activities is posted online and publicly accessible through IC on the Record (www.icontherecord.tumblr.com), the ODNI's public website dedicated to fostering greater public visibility into the intelligence activities of the government.

In January 2014, President Obama gave a speech outlining various reforms to U.S. signals intelligence activities, and issued Presidential Policy Directive 28 (PPD-28) concerning those activities.[2] The President emphasized that U.S. signals intelligence activities help secure not only our country and our freedoms, but also the security and freedoms of other countries, including EU Member States, that rely on the information U.S. intelligence agencies obtain to protect their own citizens.

PPD-28 sets out a series of principles and requirements that apply to all U.S. signals intelligence activities and for all people, regardless of nationality or location. In particular, it sets certain requirements for procedures to address the collection, retention, and dissemination of personal information about non-U.S. persons acquired pursuant to U.S. signals intelligence. These requirements are set forth in more detail below, but in summary:

- The PPD reiterates that the United States collects signals intelligence only as authorized by statute, executive order, or other Presidential directive.
- The PPD establishes procedures to ensure that signals intelligence activity is conducted only in furtherance of legitimate and authorized national security purposes.
- The PPD also requires that privacy and civil liberties be integral concerns in the planning of signals intelligence collection activities. In particular, the United States does not collect intelligence to suppress or burden criticism or dissent; in order to disadvantage persons based on their ethnicity, race, gender, sexual orientation, or religion; or to afford a competitive commercial advantage to U.S. companies and U.S. business sectors.
- The PPD directs that signals intelligence collection be as tailored as feasible and that signals intelligence collected in bulk can only be used for specific enumerated purposes.
- The PPD directs that the Intelligence Community adopt procedures "reasonably designed to minimize the dissemination and retention of personal information collected from signals intelligence activities," and in particular extending certain protections afforded to the personal information of U.S. persons to non-US person information.
- Agency procedures implementing PPD-28 have been adopted and made public.

The applicability of the procedures and protections set out herein to the Privacy Shield is clear. When data has been transferred to corporations in the United States pursuant to the Privacy Shield, or indeed by any means, U.S. intelligence agencies can seek that data from those corporations only if the request complies with FISA or is made pursuant to one of the National Security Letter statutory provisions, which are discussed below.[3] In addition, without confirming or denying media reports alleging that the U.S. Intelligence Community collects data from transatlantic cables while it is being transmitted to the United States, were the U.S. Intelligence Community to collect data from transatlantic cables, it would do so subject to the limitations and safeguards set out herein, including the requirements of PPD-28.

---

[2] *Available at* https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

[3] Law enforcement or regulatory agencies may request information from corporations for investigative purposes in the United States pursuant to other criminal, civil, and regulatory authorities that are beyond the scope of this paper, which is limited to national security authorities.

b. Collection Limitations

PPD-28 sets out a number of important general principles that govern the collection of signals intelligence:

- The collection of signals intelligence must be authorized by statute or Presidential authorization, and must be undertaken in accordance with the Constitution and law.
- Privacy and civil liberties must be integral considerations in planning signals intelligence activities.
- Signals intelligence will be collected only when there is a valid foreign intelligence or counterintelligence purpose.
- The United States will not collect signals intelligence for the purpose of suppressing or burdening criticism or dissent.
- The United States will not collect signals intelligence to disadvantage people based on their ethnicity, race, gender, sexual orientation, or religion.
- The United States will not collect signals intelligence to afford a competitive commercial advantage to U.S. companies and business sectors.
- U.S. signals intelligence activity must *always* be as tailored as feasible, taking into account the availability of other sources of information. This means, among other things, that whenever practicable, signals intelligence collection activities are conducted in a targeted manner rather than in bulk.

The requirement that signals intelligence activity be "as tailored as feasible" applies to the manner in which signals intelligence is collected, as well as to what is actually collected. For example, in determining whether to collect signals intelligence, the Intelligence Community must consider the availability of other information, including diplomatic or public sources, and prioritize collection through those means, where appropriate and feasible. Moreover, Intelligence Community element policies should require that wherever practicable, collection should be focused on specific foreign intelligence targets or topics through the use of discriminants (*e.g.*, specific facilities, selection terms and identifiers).

It is important to view the information provided to the Commission as a whole. Decisions about what is "feasible" or "practicable" are not left to the discretion of individuals but are subject to the policies that agencies have issued under PPD-28 – which have been made publicly available – and to the other processes described therein.[4] As PPD-28 says, bulk collection of signals intelligence is collection that "due to technical or operational considerations, is acquired without the use of discriminants (*e.g.*, specific identifiers, selection terms, etc.)." In this respect, PPD-28 recognizes that Intelligence community elements must collect bulk signals intelligence in certain circumstances in order to identify new or emerging threats and other vital national security information that is often hidden within the large and complex system of modern global communications. It also recognizes the privacy and civil liberties concerns raised when bulk signals intelligence is collected. PPD-28 therefore directs the Intelligence Community to prioritize alternatives that would allow the conduct of targeted signals intelligence rather than bulk signals intelligence collection. Accordingly, Intelligence Community elements should conduct targeted signals

[4] *Available at* www.icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#ppd-28. These procedures implement the targeting and tailoring concepts discussed in this letter in a manner specific to each IC element.

intelligence collection activities rather than bulk signal intelligence collection activities whenever practicable.[5] These principles ensure that the exception for bulk collection will not swallow the general rule.

As for the concept of "reasonableness," it is a bedrock principle of U.S. law. It signifies that Intelligence Community elements will not be required to adopt any measure theoretically possible, but rather will have to balance their efforts to protect legitimate privacy and civil liberties interests with the practical necessities of signals intelligence activities. Here again, the agencies' policies have been made available, and can provide assurance that the term "reasonably designed to minimize the dissemination and retention of personal information" does not undermine the general rule.

PPD-28 also provides that signals intelligence collected in bulk can only be used for six specific purposes: detecting and countering certain activities of foreign powers; counterterrorism; counter-proliferation; cybersecurity; detecting and countering threats to U.S. or allied armed forces; and combating transnational criminal threats, including sanctions evasion. The President's National Security Advisor, in consultation with the Director for National Intelligence (DNI), will annually review these permissible uses of signals intelligence collected in bulk to see whether they should be changed. The DNI will make this list publicly available to the maximum extent feasible, consistent with national security. This provides an important and transparent limitation on the use of bulk signals intelligence collection.

Additionally, the Intelligence Community elements implementing PPD-28 have reinforced existing analytic practices and standards for querying unevaluated signals intelligence.[6] Analysts must structure their queries or other search terms and techniques to ensure that they are appropriate to identify intelligence information relevant to a valid foreign intelligence or law enforcement task. To that end, IC elements must focus queries about persons on the categories of signals intelligence information responsive to a foreign intelligence or law enforcement requirement, so as to prevent the use of personal information not pertinent to foreign intelligence or law enforcement requirements.

It is important to emphasize that any bulk collection activities regarding Internet communications that the U.S. Intelligence Community performs through signals intelligence operate on a small proportion of the Internet. Additionally, the use of targeted queries, as described above, ensures that only those items believed to be of potential intelligence value are ever presented for analysts to examine. These limits are intended to protect the privacy and civil liberties of all persons, whatever their nationality and regardless of where they might reside.

The United States has elaborate processes to ensure that signals intelligence activities are conducted only in furtherance of appropriate national security purposes. Each year the President sets the nation's highest priorities for foreign intelligence collection after an extensive, formal interagency process. The DNI is responsible for translating these

---

[5] To cite but one example, the NSA's procedures implementing PPD-28 state that "[w]henever practicable, collection will occur through the use of one or more selection terms in order to focus the collection on specific foreign intelligence targets (*e.g.*, a specific, known international terrorist or terrorist group) or specific foreign intelligence topics (*e.g.*, the proliferation of weapons of mass destruction by a foreign power or its agents)."

[6] *Available at* http://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf.

intelligence priorities into the National Intelligence Priorities Framework, or NIPF. PPD-28 strengthened and enhanced the interagency process to ensure that all of the IC's intelligence priorities are reviewed and approved by high-level policymakers. Intelligence Community Directive (ICD) 204 provides further guidance on the NIPF and was updated in January 2015 to incorporate the requirements of PPD-28.[7] Although the NIPF is classified, information related to specific U.S. foreign intelligence priorities is reflected annually in the DNI's unclassified *Worldwide Threat Assessment*, which is also readily available on the ODNI website.

The priorities in the NIPF are at a fairly high level of generality. They include topics such as the pursuit of nuclear and ballistic missile capabilities by particular foreign adversaries, the effects of drug cartel corruption, and human rights abuses in specific countries. And they apply not just to signals intelligence, but to all intelligence activities. The organization that is responsible for translating the priorities in the NIPF into actual signals intelligence collection is called the National Signals Intelligence Committee, or SIGCOM. It operates under the auspices of the Director of the National Security Agency (NSA), who is designated by Executive Order 12333 as the "functional manager for signals intelligence," responsible for overseeing and coordinating signals intelligence across the Intelligence Community under the oversight of both the Secretary of Defense and the DNI. The SIGCOM has representatives from all elements of the IC and, as the United States fully implements PPD-28, also will have full representation from other departments and agencies with a policy interest in signals intelligence.

All U.S. departments and agencies that are consumers of foreign intelligence submit their requests for collection to the SIGCOM. The SIGCOM reviews those requests, ensures that they are consistent with the NIPF, and assigns them priorities using criteria such as:

- Can signals intelligence provide useful information in this case, or are there better or more cost-effective sources of information to address the requirement, such as imagery or open source information?
- How critical is this information need? If it is a high priority in the NIPF, it will most often be a high signal intelligence priority.
- What type of signals intelligence could be used?
- Is the collection as tailored as feasible? Should there be time, geographic, or other limitations?

The U.S. signals intelligence requirements process also requires explicit consideration of other factors, namely:

- Is the target of the collection, or the methodology used to collect, particularly sensitive? If so, it will require review by senior policymakers.
- Will the collection present an unwarranted risk to privacy and civil liberties, regardless of nationality?
- Are additional dissemination and retention safeguards necessary to protect privacy or national security interests?

[7] *Available at* http://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf.

Finally, at the end of the process, trained NSA personnel take the priorities validated by the SIGCOM and research and identify specific selection terms, such as telephone numbers or email addresses, which are expected to collect foreign intelligence responsive to these priorities. Any selector must be reviewed and approved before it is entered into NSA's collection systems. Even then, however, whether and when actual collection takes place will depend in part on additional considerations such as the availability of appropriate collection resources. This process ensures that U.S. signals intelligence collection targets reflect valid and important foreign intelligence needs. And, of course, when collection is conducted pursuant to FISA, NSA and other agencies must follow additional restrictions approved by the Foreign Intelligence Surveillance Court. In short, neither NSA nor any other U.S. intelligence agency decides on its own what to collect.

Overall, this process ensures that all U.S. intelligence priorities are set by senior policymakers who are in the best position to identify U.S. foreign intelligence requirements, and that those policymakers take into account not only the potential value of the intelligence collection but also the risks associated with that collection, including the risks to privacy, national economic interests, and foreign relations.

With respect to data transmitted to the United States pursuant to the Privacy Shield, although the United States cannot confirm or deny specific intelligence methods or operations, the requirements of PPD-28 apply to any signals intelligence operations the United States conducts, regardless of the type or source of data that is being collected. Further, the limitations and safeguards applicable to the collection of signals intelligence apply to signals intelligence collected for any authorized purpose, including both foreign relations and national security purposes.

The procedures discussed above demonstrate a clear commitment to prevent arbitrary and indiscriminate collection of signals intelligence information, and to implement – from the highest levels of our Government – the principle of reasonableness. PPD-28 and agency implementing procedures clarify new and existing limitations to and describe with greater specificity the purpose for which the United States collects and uses signals intelligence. These should provide assurance that signals intelligence activities are and will continue to be conducted only to further legitimate foreign intelligence goals.

c. Retention and Dissemination Limitations

Section 4 of PPD-28 requires that each element of the Intelligence Community have express limits on the retention and dissemination of personal information about non-U.S. persons collected by signals intelligence, comparable to the limits for U.S. persons. These rules are incorporated into procedures for each IC agency that were released in February 2015 and are publicly available. To qualify for retention or dissemination as foreign intelligence, personal information must relate to an authorized intelligence requirement, as determined in the NIPF process described above; be reasonably believed to be evidence of a crime; or meet one of the other standards for retention of U.S. person information identified in Executive Order 12333, section 2.3.

Information for which no such determination has been made may not be retained for more than five years, unless the DNI expressly determines that continued retention is in the national security interests of the United States. Thus, IC elements must delete non-U.S. person information collected through signals intelligence five years after collection, unless, for example, the information has been determined to be relevant to an authorized foreign

intelligence requirement, or if the DNI determines, after considering the views of the ODNI Civil Liberties Protection Officer and agency privacy and civil liberties officials, that continued retention is in the interest of national security.

In addition, all agency policies implementing PPD-28 now explicitly require that information about a person may not be disseminated solely because an individual is a non-U.S. person, and ODNI has issued a directive to all IC elements[8] to reflect this requirement. Intelligence Community personnel are specifically required to consider the privacy interests of non-U.S. persons when drafting and disseminating intelligence reports. In particular, signals intelligence about the routine activities of a foreign person would not be considered foreign intelligence that could be disseminated or retained permanently by virtue of that fact alone unless it is otherwise responsive to an authorized foreign intelligence requirement. This recognizes an important limitation and is responsive to European Commission concerns about the breadth of the definition of foreign intelligence as set forth in Executive Order 12333.

d. Compliance and Oversight

The U.S. system of foreign intelligence oversight provides rigorous and multi-layered oversight to ensure compliance with applicable laws and procedures, including those pertaining to the collection, retention, and dissemination of non-U.S. person information acquired by signals intelligence as set forth in PPD-28. These include:

- The Intelligence Community employs hundreds of oversight personnel. NSA alone has over 300 people dedicated to compliance, and other elements also have oversight offices. In addition, the Department of Justice provides extensive oversight of intelligence activities, and oversight is also provided by the Department of Defense.
- 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. 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. While Inspector General recommendations are non-binding, the Inspector General's reports are often made public, and in any event are provided to Congress; this includes follow-up reports in case corrective action recommended in previous reports has not yet been completed. Congress is therefore informed of any non-compliance and can exert pressure, including through budgetary means, to achieve corrective action. A number of Inspector General reports about intelligence programs have been publicly released.[9]
- ODNI's Civil Liberties and Privacy Office (CLPO) is charged with ensuring that the IC operates in a manner that advances national security while protecting civil liberties and privacy rights.[10] Other IC elements have their own privacy officers.
- The Privacy and Civil Liberties Oversight Board (PCLOB), an independent body established by statute, is charged with analyzing and reviewing counterterrorism programs and policies, including the use of signals intelligence, to ensure that they

[8] Intelligence Community Directive (ICD) 203, *available at* http://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.
[9] *See, e.g.,* U.S. Department of Justice Inspector General Report "A Review of the Federal Bureau of Investigation's Activities Under Section 702 of the Foreign Intelligence Surveillance Act of 2008" (September 2012), *available at* https://oig.justice.gov/reports/2016/o1601a.pdf.
[10] *See* www.dni.gov/clpo.

adequately protect privacy and civil liberties. It has issued several public reports on intelligence activities.

- As discussed more fully below, the Foreign Intelligence Surveillance Court, a court composed of independent federal judges, is responsible for oversight and compliance of any signals intelligence collection activities conducted pursuant to FISA.
- Finally, the U.S. Congress, specifically the House and Senate Intelligence and Judiciary Committees, have significant oversight responsibilities regarding all U.S. foreign intelligence activities, including U.S. signals intelligence.

Apart from these formal oversight mechanisms, the Intelligence Community has in place numerous mechanisms to ensure that the Intelligence Community is complying with the limitations on collection described above. For example:

- Cabinet officials are required to validate their signals intelligence requirements each year.
- NSA checks signals intelligence targets throughout the collection process to determine if they are actually providing valuable foreign intelligence responsive to the priorities, and will stop collection against targets that are not. Additional procedures ensure that selection terms are reviewed periodically.
- Based on a recommendation from an independent Review Group appointed by President Obama, the DNI has established a new mechanism to monitor the collection and dissemination of signals intelligence that is particularly sensitive because of the nature of the target or the means of collection, to ensure that it is consistent with the determinations of policymakers.
- Finally, ODNI annually reviews the IC's allocation of resources against the NIPF priorities and the intelligence mission as a whole. This review includes assessments of the value of all types of intelligence collection, including signals intelligence, and looks both backward – how successful has the IC been in achieving its goals? – and forward – what will the IC need in the future? This ensures that signals intelligence resources are applied to the most important national priorities.

As evidenced by this comprehensive overview, the Intelligence Community does not decide on its own which conversations to listen to, try to collect everything, or operate free from scrutiny. Its activities are focused on priorities set by policymakers, through a process that involves input from across the government, and that is overseen both within NSA and by the ODNI, Department of Justice, and Department of Defense.

PPD-28 also contains numerous other provisions to ensure that personal information collected pursuant to signals intelligence is protected, regardless of nationality. For instance, PPD-28 provides for data security, access, and quality procedures to protect personal information collected through signals intelligence, and provides for mandatory training to ensure that the workforce understands the responsibility to protect personal information, regardless of nationality. The PPD also provides for additional oversight and compliance mechanisms. These include periodic audit and reviews by appropriate oversight and compliance officials of the practices for protecting personal information contained in signals intelligence. The reviews also must examine the agencies' compliance with the procedures for protecting such information.

Additionally, PPD-28 provides that significant compliance issues related to non-U.S. persons will be addressed at senior levels of government. Should a significant compliance

issue occur involving the personal information of any person collected as a result of signals intelligence activities, the issue must, in addition to any existing reporting requirements, be reported promptly to the DNI. If the issue involves the personal information of a non-U.S. person, the DNI, in consultation with the Secretary of State and the head of the relevant IC element, will determine whether steps should be taken to notify the relevant foreign government, consistent with the protection of sources and methods and of U.S. personnel. Moreover, as directed by PPD-28, the Secretary of State has identified a senior official, Under Secretary Catherine Novelli, to serve as a point of contact for foreign governments that wish to raise concerns regarding signals intelligence activities of the United States. This commitment to high-level engagement exemplifies the efforts the U.S. government has made over the past few years to instill confidence in the numerous and overlapping privacy protections in place for U.S. person and non-U.S. person information.

e. ***Summary***

The United States' processes for collecting, retaining, and disseminating foreign intelligence provide important privacy protections for the personal information of all persons, regardless of nationality. In particular, these processes ensure that our Intelligence Community focuses on its national security mission as authorized by applicable laws, executive orders, and presidential directives; safeguards information from unauthorized access, use and disclosure; and conducts its activities under multiple layers of review and oversight, including by congressional oversight committees. PPD-28 and the procedures implementing it represent our efforts to extend certain minimization and other substantial data protection principles to the personal information of all persons regardless of nationality. Personal information obtained through U.S. signals intelligence collection is subject to the principles and requirements of U.S. law and Presidential direction, including the protections set forth in PPD-28. These principles and requirements ensure that all persons are treated with dignity and respect, regardless of their nationality or wherever they might reside, and recognize that all persons have legitimate privacy interests in the handling of their personal information.

II. Foreign Intelligence Surveillance Act – Section 702

Collection under Section 702 of the Foreign Intelligence Surveillance Act[11] is not "mass and indiscriminate" but is narrowly focused on the collection of foreign intelligence from individually identified legitimate targets; is clearly authorized by explicit statutory authority; and is subject to both independent judicial supervision and substantial review and oversight within the Executive Branch and Congress. Collection under Section 702 is considered signals intelligence subject to the requirements of PPD-28.[12]

---

[11] 50 U.S.C. § 1881a.

[12] The United States also may obtain court orders pursuant to other provisions of FISA for the production of data, including data transferred pursuant to the Privacy Shield. *See* 50 U.S.C. § 1801 *et seq*. Titles I and III of FISA, which respectively authorize electronic surveillance and physical searches, require a court order (except in emergency circumstances) and always require probable cause to believe that the target is a foreign power or an agent of a foreign power. Title IV of FISA authorizes the use of pen registers and trap and trace devices, pursuant to court order (except in emergency circumstances) in authorized foreign intelligence, counterintelligence, or counterterrorism investigations. Title V of FISA permits the FBI, pursuant to court order (except in emergency circumstances), to obtain business records that are relevant to an authorized foreign intelligence, counterintelligence, or counterterrorism investigations. As discussed below, the USA FREEDOM Act specifically prohibits the use of FISA pen register or business

Collection under Section 702 is one of the most valuable sources of intelligence protecting both the United States and our European partners. Extensive information about the operation and oversight of Section 702 is publicly available. Numerous court filings, judicial decisions and oversight reports relating to the program have been declassified and released on the ODNI's public disclosure website, www.icontherecord.tumblr.com. Moreover, Section 702 was comprehensively analyzed by the PCLOB, in a report which is available at https://www.pclob.gov/library/702-Report.pdf.[13]

Section 702 was passed as part of the FISA Amendments Act of 2008,[14] after extensive public debate in Congress. It authorizes the acquisition of foreign intelligence information through targeting of non-U.S. persons located outside the United States, with the compelled assistance of U.S. electronic communications service providers. Section 702 authorizes the Attorney General and the DNI – two Cabinet-level officials appointed by the President and confirmed by the Senate – to submit annual certifications to the FISA Court.[15] These certifications identify specific categories of foreign intelligence to be collected, such as intelligence related to counterterrorism or weapons of mass destruction, which must fall within the categories of foreign intelligence defined by the FISA statute.[16] As the PCLOB noted, "[t]hese limitations do *not* permit unrestricted collection of information about foreigners."[17]

The certifications also are required to include "targeting" and "minimization" procedures that must be reviewed and approved by the FISA Court.[18] The targeting procedures are designed to ensure that the collection takes place only as authorized by statute and is within the scope of the certifications; the minimization procedures are designed to limit the acquisition, dissemination, and retention of information about U.S. persons, but also contain provisions that provide substantial protection to information about non-U.S. persons as well, described below. Moreover, as described above, in PPD-28 the President directed that the Intelligence Community provide additional protections for personal information about non-U.S. persons, and those protections apply to information collected under Section 702.

Once the court approves the targeting and minimization procedures, collection under Section 702 is not bulk or indiscriminate, but "consists entirely of targeting specific persons about whom an individualized determination has been made," as the PCLOB said.[19] Collection is targeted through the use of individual selectors, such as email addresses or telephone numbers, which U.S. intelligence personnel have determined are likely being used to communicate foreign intelligence information of the type covered by the certification submitted to the court.[20] The basis for selection of the target must be documented, and the

---

record orders for bulk collection, and imposes a requirement of a "specific selection term" to ensure that those authorities are used in a targeted fashion.

[13] Privacy and Civil Liberties Board, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act" (July 2, 2014) ("PCLOB Report").

[14] *See* Pub. L. No. 110-261, 122 Stat. 2436 (2008).

[15] *See* 50 U.S.C. § 1881a(a) and (b).

[16] *See id.* § 1801(e).

[17] *See* PCLOB Report at 99.

[18] *See* 50 U.S.C. § 1881a(d) and (e).

[19] *See* PCLOB Report at 111.

[20] *Id.*

documentation for every selector is subsequently reviewed by the Department of Justice.[21] The U.S. Government has released information showing that in 2014 there were approximately 90,000 individuals targeted under Section 702, a miniscule fraction of the over 3 billion internet users throughout the world.[22]

Information collected under Section 702 is subject to the court-approved minimization procedures, which provide protections to non-U.S. persons as well as U.S. persons, and which have been publicly released.[23] For example, communications acquired under Section 702, whether of U.S. persons or non-U.S. persons, are stored in databases with strict access controls. They may be reviewed only by intelligence personnel who have been trained in the privacy-protective minimization procedures and who have been specifically approved for that access in order to carry out their authorized functions.[24] Use of the data is limited to identification of foreign intelligence information or evidence of a crime.[25] Pursuant to PPD-28, this information may be disseminated only if there is a valid foreign intelligence or law enforcement purpose; the mere fact that one party to the communication is not a U.S. person is not sufficient.[26] And the minimization procedures and PPD-28 also set limits on how long data acquired pursuant to Section 702 may be retained.[27]

Oversight of Section 702 is extensive, and is conducted by all three branches of our government. Agencies implementing the statute have multiple levels of internal review, including by independent Inspectors General, and technological controls over access to the data. The Department of Justice and the ODNI closely review and scrutinize the use of Section 702 to verify compliance with legal rules; agencies are also under an independent obligation to report potential incidents of noncompliance. Those incidents are investigated, and all compliance incidents are reported to the Foreign Intelligence Surveillance Court, the President's Intelligence Oversight Board, and Congress, and remedied as appropriate.[28] To date, there have been no incidents of willful attempts to violate the law or circumvent legal requirements.[29]

---

[21] *Id.* at 8; 50 U.S.C. § 1881a(l); *see also* NSA Director of Civil Liberties and Privacy Report, "NSA's Implementation of Foreign Intelligence Surveillance Act Section 702" (hereinafter "NSA Report") at 4, *available at* http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

[22] Director of National Intelligence 2014 Transparency Report, *available at* http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014.

[23] Minimization procedures available at: http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf ("NSA Minimization Procedures"); http://www.dni.gov/files/documents/ppd-28/2014%20FBI%20702%20Minimization%20Procedures.pdf; and http://www.dni.gov/files/documents/ppd-28/2014%20CIA%20702%20Minimization%20Procedures.pdf.

[24] *See* NSA Report at 4.

[25] *See, e.g.,* NSA Minimization Procedures at 6.

[26] Intelligence Agency PPD-28 procedures available at http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

[27] *See* NSA Minimization Procedures; PPD-28 Section 4.

[28] *See* 50 U.S.C. § 1881(l); *see also* PCLOB Report at 66-76.

[29] *See* Semiannual Assessment of Compliance with Procedures and Guidelines Issues Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence at 2–3, *available at* http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf.

The FISA Court plays an important role in implementing Section 702. It is composed of independent federal judges who serve for a term of seven years on the FISA Court but who, like all federal judges, have life tenure as judges. As noted above, the Court must review the annual certifications and targeting and minimization procedures for compliance with the law. In addition, as also noted above, the Government is required to notify the Court immediately of compliance issues,[30] and several Court opinions have been declassified and released showing the exceptional degree of judicial scrutiny and independence it exercises in reviewing those incidents.

The Court's exacting processes have been described by its former Presiding Judge in a letter to Congress that has been publicly released.[31] And as a result of the USA FREEDOM Act, described below, the Court is now explicitly authorized to appoint an outside lawyer as an independent advocate on behalf of privacy in cases that present novel or significant legal issues.[32] This degree of involvement by a country's independent judiciary in foreign intelligence activities directed at persons who are neither citizens of that country nor located within it is unusual if not unprecedented, and helps ensure that Section 702 collection occurs within appropriate legal limits.

Congress exercises oversight through statutorily required reports to the Intelligence and Judiciary Committees, and frequent briefings and hearings. These include a semiannual report by the Attorney General documenting the use of Section 702 and any compliance incidents; [33] a separate semiannual assessment by the Attorney General and the DNI documenting compliance with the targeting and minimization procedures, including compliance with the procedures designed to ensure that collection is for a valid foreign intelligence purpose;[34] and an annual report by heads of intelligence elements which includes a certification that collection under Section 702 continues to produce foreign intelligence information.[35]

In short, collection under Section 702 is authorized by law; subject to multiple levels of review, judicial supervision and oversight; and, as the FISA Court stated in a recently declassified opinion, is "not conducted in a bulk or indiscriminate manner," but "through . . . discrete targeting decisions for individual [communication] facilities."[36]

III. USA FREEDOM Act

The USA FREEDOM Act, signed into law in June 2015, significantly modified U.S. surveillance and other national security authorities, and increased public transparency on the use of these authorities and on decisions of the FISA Court, as set out below. [37] The Act ensures that our intelligence and law enforcement professionals have the authorities they need

---

[30] Rule 13 of the Foreign Intelligence Surveillance Court Rules of Procedures, *available at* http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.
[31] July 29, 2013 Letter from The Honorable Reggie B. Walton to The Honorable Patrick J. Leahy, *available at* http://fas.org/irp/news/2013/07/fisc-leahy.pdf.
[32] *See* Section 401 of the USA FREEDOM Act, P.L. 114-23.
[33] *See* 50 U.S.C. § 1881f.
[34] *See id.* § 1881a(l)(1).
[35] *See id.* § 1881a(l)(3). Some of these reports are classified.
[36] Mem. Opinion and Order at 26 (FISC 2014), a*vailable at* http://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.
[37] *See* USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 401, 129 Stat. 268.

to protect the Nation, while further ensuring that individuals' privacy is appropriately protected when these authorities are employed. It enhances privacy and civil liberties and increases transparency.

The Act prohibits bulk collection of any records, including of both U.S. and non-U.S. persons, pursuant to various provisions of FISA or through the use of National Security Letters, a form of statutorily authorized administrative subpoenas.[38] This prohibition specifically includes telephone metadata relating to calls between persons inside the U.S. and persons outside the U.S., and would also include collection of Privacy Shield information pursuant to these authorities. The Act requires that the government base any application for records under those authorities on a "specific selection term"—a term that specifically identifies a person, account, address, or personal device in a way that limits the scope of information sought to the greatest extent reasonably practicable.[39] This further ensures that collection of information for intelligence purposes is precisely focused and targeted.

The Act also made significant modifications to proceedings before the FISA Court, which both increase transparency and provide additional assurances that privacy will be protected. As noted above, it authorized creation of a standing panel of security-cleared lawyers with expertise in privacy and civil liberties, intelligence collection, communications technology, or other relevant areas, who may be appointed to appear before the court as *amicus curiae* in cases that involve significant or novel interpretations of law. These lawyers are authorized to make legal arguments that advance the protection of individual privacy and civil liberties, and will have access to any information, including classified information, that the court determines is necessary to their duties.[40]

The Act also builds on the U.S. Government's unprecedented transparency about intelligence activities by requiring the DNI, in consultation with the Attorney General, to either declassify, or publish an unclassified summary of, each decision, order, or opinion issued by the FISA Court or the Foreign Intelligence Surveillance Court of Review that includes a significant construction or interpretation of any provision of law.

Moreover, the Act provides for extensive disclosures about FISA collection and National Security Letter requests. The United States must disclose to Congress and to the public each year the number of FISA orders and certifications sought and received; estimates of the number of U.S. persons and non-U.S. persons targeted and affected by surveillance; and the number of appointments of *amici curiae*, among other items of information.[41] The

[38] *See id.* §§ 103, 201, 501. National Security Letters are authorized by a variety of statutes and allow the FBI to obtain information contained in credit reports, financial records, and electronic subscriber and transaction records from certain kinds of companies, only to protect against international terrorism or clandestine intelligence activities. *See* 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u-1681v; 18 U.S.C. § 2709. National Security Letters are typically used by the FBI to gather critical non-content information at the early phases of counterterrorism and counterintelligence investigations – such as the identity of the subscriber to an account who may have been communicating with agents of a terrorist group such as ISIL. Recipients of a National Security Letter have the right to challenge them in court. *See* 18 U.S.C. § 3511.

[39] *See id.*

[40] *See id.* § 401.

[41] *See id.* § 602.

Act also requires additional public reporting by the government about the numbers of National Security Letter requests about both U.S. and non-U.S. persons.[42]

With regard to corporate transparency, the Act gives companies a range of options to report publicly the aggregate number of FISA orders and directives or National Security Letters they receive from the Government, as well as the number of customer accounts targeted by these orders.[43] Several companies have already made such disclosures, which have revealed the limited number of customers whose records have been sought.

These corporate transparency reports demonstrate that U.S. intelligence requests affect only a miniscule fraction of data. For example, one major company's recent transparency report shows that it received national security requests (pursuant to FISA or National Security Letters) affecting fewer than 20,000 of its accounts, at a time when it had at least 400 million subscribers. In other words, all U.S. national security requests reported by this company affected fewer than .005% of its subscribers. Even if every one of those requests had concerned Safe Harbor data, which of course is not the case, it is obvious that the requests are targeted and appropriate in scale, and are neither bulk nor indiscriminate.

Finally, while the statutes which authorize National Security Letters already restricted the circumstances under which a recipient of such a letter could be barred from disclosing it, the Act further provided that such non-disclosure requirements must be reviewed periodically; required that recipients of National Security Letters be notified when the facts no longer support a non-disclosure requirement; and codified procedures for recipients to challenge nondisclosure requirements.[44]

In sum, the USA FREEDOM Act's important amendments to U.S. intelligence authorities is clear evidence of the extensive effort taken by the United States to place the protection of personal information, privacy, civil liberties, and transparency at the forefront of all U.S. intelligence practices.

IV. Transparency

In addition to the transparency mandated by the USA FREEDOM Act, the U.S. Intelligence Community provides the public much additional information, setting a strong example with respect to transparency into its intelligence activities. The Intelligence Community has published many of its policies, procedures, Foreign Intelligence Surveillance Court decisions, and other declassified materials, providing an extraordinary degree of transparency. In addition, the Intelligence Community has substantially increased its disclosure of statistics on the government's use of national security collection authorities. On April 22, 2015, the Intelligence Community issued its second annual report presenting statistics on how often the government uses these important authorities. ODNI also has published, on the ODNI website and on *IC On the Record*, a set of concrete transparency principles[45] and an implementation plan that translates the principles into concrete,

---

[42] *See id.*
[43] *See id.* § 603.
[44] *See id.* §§ 502(f)–503.
[45] *Available at* http:\\www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles.

measurable initiatives.[46] In October 2015, the Director of National Intelligence directed that each intelligence agency designate an Intelligence Transparency Officer within its leadership to foster transparency and lead transparency initiatives.[47] The Transparency Officer will work closely with each intelligence agency's Privacy and Civil Liberties Officer to ensure that transparency, privacy, and civil liberties continue to remain top priorities.

As an example of these efforts, NSA's Chief Privacy and Civil Liberties Officer has released several unclassified reports over the past few years, including reports on activities under section 702, Executive Order 12333, and the USA FREEDOM Act.[48] In addition, the IC works closely with the PCLOB, Congress, and the U.S. privacy advocacy community to provide further transparency relating to U.S. intelligence activities, wherever feasible and consistent with the protection of sensitive intelligence sources and methods. Taken as a whole, U.S. intelligence activities are as transparent as or more transparent than those of any other nation in the world and are as transparent as it is possible to be consistent with the need to protect sensitive sources and methods.

To summarize the extensive transparency that exists about U.S. intelligence activities:

- The IC has released and posted online thousands of pages of court opinions and agency procedures outlining the specific procedures and requirements of our intelligence activities. We have also released reports on intelligence agencies' compliance with applicable restrictions.
- Senior intelligence officials regularly speak publicly about the roles and activities of their organizations, including descriptions of the compliance regimes and safeguards that govern their work.
- The IC released numerous additional documents about intelligence activities pursuant to our Freedom of Information Act.
- The President issued PPD-28, publicly setting out additional restrictions on our intelligence activities, and ODNI has issued two public reports on the implementation of those restrictions.
- The IC is now required by law to release significant legal opinions issued by the FISA Court, or summaries of those opinions.
- The government is required to report annually on the extent of its use of certain national security authorities, and companies are authorized to do so as well.
- The PCLOB has issued several detailed public reports on intelligence activities, and will continue to do so.
- The IC provides extensive classified information to Congressional oversight committees.
- The DNI issued transparency principles to govern the activities of the Intelligence Community.

---

[46] *Available at* http:\\www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Principles%20of%20Intelligence%20Transparency%20Implementation%20Plan.pdf.

[47] *See id.*

[48] *Available at* https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf.

This extensive transparency will continue going forward. Any information that is released publicly will, of course, be available to both the Department of Commerce and the European Commission. The annual review between Commerce and the European Commission on the implementation of the Privacy Shield will provide an opportunity for the European Commission to discuss any questions raised by any new information released, as well as any other matters concerning the Privacy Shield and its operation, and we understand that the Department may, in its discretion, invite representatives of other agencies, including the IC, to participate in that review. This is, of course, in addition to the mechanism provided in PPD-28 for EU Member States to raise surveillance-related concerns with a designated State Department official.

V. Redress

U.S. law provides a number of avenues of redress for individuals who have been the subject of unlawful electronic surveillance for national security purposes. Under FISA, the right to seek relief in U.S. court is not limited to U.S. persons. An individual who can establish standing to bring suit would have remedies to challenge unlawful electronic surveillance under FISA. For example, FISA allows persons subjected to unlawful electronic surveillance to sue U.S. government officials in their personal capacities for money damages, including punitive damages and attorney's fees. *See* 50 U.S.C. § 1810. Individuals who can establish their standing to sue also have a civil cause of action for money damages, including litigation costs, against the United States when information about them obtained in electronic surveillance under FISA has been unlawfully and willfully used or disclosed. *See* 18 U.S.C. § 2712. In the event the government intends to use or disclose any information obtained or derived from electronic surveillance of any aggrieved person under FISA against that person in judicial or administrative proceedings in the United States, it must provide advance notice of its intent to the tribunal and the person, who may then challenge the legality of the surveillance and seek to suppress the information. *See* 50 U.S.C. § 1806. Finally, FISA also provides criminal penalties for individuals who intentionally engage in unlawful electronic surveillance under color of law or who intentionally use or disclose information obtained by unlawful surveillance. *See* 50 U.S.C. § 1809.

EU citizens have other avenues to seek legal recourse against U.S. government officials for unlawful government use of or access to data, including government officials who violate the law in the course of unlawful access to or use of information for purported national security purposes. The Computer Fraud and Abuse Act prohibits intentional unauthorized access (or exceeding authorized access) to obtain information from a financial institution, a U.S. government computer system, or a computer accessed via the Internet, as well as threats to damage protected computers for purposes of extortion or fraud. *See* 18 U.S.C. § 1030. Any person, of whatever nationality, who suffers damage or loss by reason of a violation of this law may sue the violator (including a government official) for compensatory damages and injunctive or other equitable relief under section 1030(g), regardless of whether a criminal prosecution has been pursued, provided the conduct involves at least one of several circumstances set forth in the statute. The Electronic Communications Privacy Act (ECPA) regulates government access to stored electronic communications and transactional records and subscriber information held by third-party communications providers. *See* 18 U.S.C. §§ 2701-2712. ECPA authorizes an aggrieved individual to sue government officials for intentional unlawful access to stored data. ECPA applies to all persons regardless of citizenship and aggrieved persons may receive damages and attorney's fees. The Right to Financial Privacy Act (RFPA) limits the U.S. government's access to the bank and broker-dealer records of individual customers. *See* 12 U.S.C. §§ 3401-3422. Under

the RFPA, a bank or broker-dealer customer can sue the U.S. government for statutory, actual, and punitive damages for wrongfully obtaining access to the customer's records, and a finding that such wrongful access was willful automatically triggers an investigation of possible disciplinary action against the relevant government employees. *See* 12 U.S.C. § 3417.

Finally, the Freedom of Information Act (FOIA) provides a means for any person to seek access to existing federal agency records on any topic subject to certain categories of exemptions. *See* 5 U.S.C. § 552(b). These include limits on access to classified national security information, personal information of other individuals, and information concerning law enforcement investigations, and are comparable to the limitations imposed by nations with their own information access laws. These limitations apply equally to Americans and non-Americans. 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.[49] Although no monetary damages are available, courts can award attorney's fees.

VI. Conclusion

The United States recognizes that our signals intelligence and other intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or place of residence, and that all persons have legitimate privacy interests in the handling of their personal information. The United States only uses signals intelligence to advance its national security and foreign policy interests and to protect its citizens and the citizens of its allies and partners from harm. In short, the IC does not engage in indiscriminate surveillance of anyone, including ordinary European citizens. Signals intelligence collection only takes place when duly authorized and in a manner that strictly complies with these limitations; only after consideration of the availability of alternative sources, including from diplomatic and public sources; and in a manner that prioritizes appropriate and feasible alternatives. And wherever practicable, signals intelligence only takes place through collection focused on specific foreign intelligence targets or topics through the use of discriminants.

U.S. policy in this regard was affirmed in PPD-28. Within this framework, U.S. intelligence agencies do not have the legal authority, the resources, the technical capability or the desire to intercept all of the world's communications. Those agencies are not reading the emails of everyone in the United States, or of everyone in the world. Consistent with PPD-28, the United States provides robust protections to the personal information of non-U.S. persons that is collected through signals intelligence activities. To the maximum extent feasible consistent with the national security, this includes policies and procedures to minimize the retention and dissemination of personal information concerning non-U.S. persons comparable to the protections enjoyed by U.S. persons. Moreover, as discussed above, the comprehensive oversight regime of the targeted Section 702 FISA authority is unparalleled. Finally, the significant amendments to U.S. intelligence law set forth in the USA FREEDOM Act and the ODNI-led initiatives to promote transparency within the

[49] *See, e.g., New York Times v. Department of Justice*, 756 F.3d 100 (2d Cir. 2014); *American Civil Liberties Union v. CIA*, 710 F.3d 422 (D.C. Cir. 2014).

Intelligence Community greatly enhance the privacy and civil liberties of all individuals, regardless of their nationality.

Sincerely,

Robert S. Litt

June 21, 2016

Mr. Justin S. Antonipillai
Counselor
U.S. Department of Commerce
1401 Constitution Avenue, N.W.
Washington, DC 20230

Mr. Ted Dean
Deputy Assistant Secretary
International Trade Administration
1401 Constitution Avenue, N.W.
Washington, DC 20230

Dear Mr. Antonipillai and Mr. Dean:

I am writing to provide further information about the manner in which the United States conducts bulk collection of signals intelligence. As explained in footnote 5 of Presidential Policy Directive 28 (PPD-28), "bulk" collection refers to the acquisition of a relatively large volume of signals intelligence information or data under circumstances where the Intelligence Community cannot use an identifier associated with a specific target (such as the target's email address or phone number) to focus the collection. However, this does not mean that this sort of collection is "mass" or "indiscriminate." Indeed, PPD-28 also requires that "[s]ignals intelligence activities shall be as tailored as feasible." In furtherance of this mandate, the Intelligence Community takes steps to ensure that even when we cannot use specific identifiers to target collection, the data to be collected is likely to contain foreign intelligence that will be responsive to requirements articulated by U.S. policy-makers pursuant to the process explained in my earlier letter, and minimizes the amount of non-pertinent information that is collected.

As an example, the Intelligence Community may be asked to acquire signals intelligence about the activities of a terrorist group operating in a region of a Middle Eastern country, that is believed to be plotting attacks against Western European countries, but may not know the names, phone numbers, email addresses or other specific identifiers of individuals associated with this terrorist group. We might choose to target that group by collecting communications to and from that region for further review and analysis to identify those communications that relate to the group. In so doing, the Intelligence Community would seek to narrow the collection as much as possible. This would be considered collection in "bulk" because the use of discriminants is not feasible, but it is neither "mass" nor "indiscriminate"; rather it is focused as precisely as possible.

Thus, even when targeting through the use of specific selectors is not possible, the United States does not collect all communications from all communications facilities everywhere in the world, but applies filters and other technical tools to focus its collection on those facilities that are likely to contain communications of foreign intelligence value. In so doing, the United States' signals intelligence activities touch only a fraction of the communications traversing the Internet.

Moreover, as noted in my earlier letter, because "bulk" collection entails a greater risk of collecting non-pertinent communications, PPD-28 limits the use that the Intelligence

Community may make of signals intelligence collected in bulk to six specified purposes. PPD-28, and agency policies implementing PPD-28, also place restrictions on the retention and dissemination of personal information acquired through signals intelligence, regardless of whether the information was collected in bulk or through targeted collection, and regardless of the individual's nationality.

Thus, the Intelligence Community's "bulk" collection is not "mass" or "indiscriminate," but involves the application of methods and tools to filter collection in order to focus the collection on material that will be responsive to policy-makers' articulated foreign intelligence requirements while minimizing the collection of non-pertinent information, and provides strict rules to protect the non-pertinent information that may be acquired. The policies and procedures described in this letter apply to all bulk signals intelligence collection, including any bulk collection of communications to and from Europe, without confirming or denying whether any such collection occurs.

You have also asked for more information about the Privacy and Civil Liberties Oversight Board (PCLOB) and Inspectors General, and their authorities. The PCLOB is an independent agency in the Executive Branch. Members of the bipartisan, five-member Board are appointed by the President and confirmed by the Senate.[1] Each Member of the Board serves a six-year term. Members of the Board and staff are provided appropriate security clearances in order for them to fully execute their statutory duties and responsibilities.[2]

The PCLOB's mission is to ensure that the federal government's efforts to prevent terrorism are balanced with the need to protect privacy and civil liberties. The Board has two fundamental responsibilities – oversight and advice. The PCLOB sets its own agenda and determines what oversight or advice activities it wishes to undertake.

In its *oversight* role, the PCLOB reviews and analyzes actions the Executive Branch takes to protect the nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties.[3] The PCLOB's most recent completed oversight review focused on surveillance programs operated under Section 702 of FISA.[4] It is currently conducting a review of intelligence activities operated under Executive Order 12333.[5]

In its *advisory* role, the PCLOB ensures that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the nation from terrorism.[6]

In order to carry out its mission, the Board is authorized by statute to have access to all relevant agency records, reports, audits, reviews, documents, papers, recommendations, and any other relevant materials, including classified information consistent with law.[7] In

[1] 42 U.S.C. 2000ee(a), (h).
[2] 42 U.S.C. 2000ee(k).
[3] 42 U.S.C. 2000ee(d)(2).
[4] *See generally* https://www.pclob.gov/library.html#oversightreports.
[5] *See generally* https://www.pclob.gov/events/2015/may13.html.
[6] 42 U.S.C. 2000ee(d)(1); *see also* PCLOB Advisory Function Policy and Procedure, Policy 2015-004, *available at* https://www.pclob.gov/library/Policy-Advisory_Function_Policy_Procedure.pdf.
[7] 42 U.S.C. 2000ee(g)(1)(A).

addition, the Board may interview, take statements from, or take public testimony from any executive branch officer or employee.[8] Additionally, the Board may request in writing that the Attorney General, on the Board's behalf, issues subpoenas compelling parties outside the Executive Branch to provide relevant information.[9]

Finally, the PCLOB has statutory public transparency requirements. This includes keeping the public informed of its activities by holding public hearings and making its reports publicly available, to the greatest extent possible consistent with the protection of classified information.[10] In addition, the PCLOB is required to report when an Executive Branch agency declines to follow its advice.

Inspectors General (IGs) in the Intelligence Community (IC) conduct audits, inspections, and reviews of the programs and activities in the IC to identify and address systemic risks, vulnerabilities, and deficiencies. In addition, IGs investigate complaints or information of allegations of violations of law, rules, or regulations, or mismanagement; gross waste of funds; abuse of authority, or a substantial and specific danger to the public health and safety in IC programs and activities. IG independence is a critical component to the objectivity and integrity of every report, finding, and recommendation an IG issues. Some of the most critical components to maintaining IG independence include the IG appointment and removal process; separate operational, budget, and personnel authorities; and dual reporting requirements to Executive Branch agency heads and Congress.

Congress established an independent IG office in each Executive Branch agency, including every IC element.[11] With the passage of the Intelligence Authorization Act for Fiscal Year 2015, almost all IGs with oversight of an IC element are appointed by the President and confirmed by the Senate, including the Department of Justice, Central Intelligence Agency, National Security Agency, and the Intelligence Community.[12] Further, these IGs are permanent, nonpartisan, officials who can only be removed by the President. While the U.S. Constitution requires that the President have IG removal authority, it has rarely been exercised and requires that the President provide Congress with a written justification 30 days before removing an IG. [13] This IG appointment process ensures that there is no undue influence by Executive Branch officials in the selection, appointment, or removal of an IG.

Second, IGs have significant statutory authorities to conduct audits, investigations, and reviews of Executive Branch programs and operations. In addition to oversight investigations and reviews required by law, IGs have broad discretion to exercise oversight

[8] 42 U.S.C. 2000ee(g)(1)(B).
[9] 42 U.S.C. 2000ee(g)(1)(D).
[10] 42 U.S.C. 2000eee(f).
[11] Sections 2 and 4 of the Inspector General Act of 1978, as amended (hereinafter "IG Act"); Section 103H(b) and (e) of the National Security Act of 1947, as amended (hereinafter "Nat'l Sec. Act"); Section 17(a) of the Central Intelligence Act (hereinafter "CIA Act").
[12] *See* Pub. L. No. 113-293, 128 Stat. 3990, (Dec. 19, 2014). Only the IGs for the Defense Intelligence Agency and the National Geospatial-Intelligence Agency are not appointed by the President; however the DOD IG and the IC IG have concurrent jurisdiction over these agencies.
[13] Section 3 of the IG Act of 1978, as amended; Section 103H(c) of the Nat'l Sec. Act; and Section 17(b) of the CIA Act.

authority to review programs and activities of their choosing.[14] In exercising this authority, the law ensures that IGs have the independent resources to execute their responsibilities, including the authority to hire their own staff and separately document their budget requests to Congress.[15] The law ensures that IGs have access to the information needed to execute their responsibilities. This includes the authority to have direct access to all agency records and information detailing the programs and operations of the agency regardless of classification; the authority to subpoena information and documents; and the authority to administer oaths.[16] In limited cases, the head of an Executive Branch agency may prohibit an IG's activity if, for example, an IG audit or investigation would significantly impair the national security interests of the United States. Again, the exercise of this authority is extremely unusual and requires the head of the agency to notify Congress within 30 days of the reasons for exercising it.[17] Indeed, the Director of National Intelligence has never exercised this limitation authority over any IG activities.

Third, IGs have responsibilities to keep both heads of Executive Branch agencies and Congress fully and currently informed through reports of fraud and other serious problems, abuses, and deficiencies relating to Executive Branch programs and activities.[18] Dual reporting bolsters IG independence by providing transparency into the IG oversight process and allowing agency heads an opportunity to implement IG recommendations before Congress can take legislative action. For example, IGs are required by law to complete semi-annual reports that describe such problems as well as corrective actions taken to date.[19] Executive Branch agencies take IG findings and recommendations seriously and IGs are often able to include the agencies' acceptance and implementation of IG recommendations in these and other reports provided to Congress, and in some cases the public.[20] In addition to this IG dual-report structure, IGs are also responsible for shepherding Executive Branch whistleblowers to the appropriate congressional oversight committees to make disclosures of alleged fraud, waste, or abuse in Executive Branch programs and activities. The identities of those who come forward are protected from disclosure to the Executive Branch, which shields the whistleblowers from potential prohibited personnel actions or security clearance actions taken in reprisal for reporting to the IG.[21] As whistleblowers are often the sources for IG investigations, the ability to report their concerns to the Congress without Executive

[14] *See* Sections 4(a) and 6(a)(2) of the IG Act of 1947; Section 103H(e) and (g)(2)(A) of the Nat'l Sec. Act; Section 17(a) and (c) of the CIA Act.
[15] Sections 3(d), 6(a)(7) and 6(f) of the IG Act; Sections 103H(d), (i), (j) and (m) of the Nat'l Sec. Act; Sections 17(e)(7) and (f) of the CIA Act.
[16] Section 6(a)(1), (3), (4), (5), and (6) of the IG Act ; Sections 103H(g)(2) of the Nat'l Sec. Act; Section 17(e)(1), (2), (4), and (5) of CIA Act.
[17] *See, e.g.*, Sections 8(b) and 8E(a) of the IG Act; Section 103H(f) of the Nat'l Sec. Act; Section 17(b) of the CIA Act.
[18] Section 4(a)(5) of the IG Act; Section 103H(a)(b)(3) and (4) of the Nat'l Sec. Act; Section 17(a)(2) and (4) of the CIA Act.
[19] Section 2(3), 4(a), and 5 of the IG Act; Section 103H(k) of the Nat'l Sec. Act; Section 17(d) of the CIA Act. The Inspector General of the Department of Justice makes its publicly released reports available on the internet at http://oig.justice.gov/reports/all.htm. Similarly, the Inspector General for the Intelligence Community makes it semi-annual reports publicly available at https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig.
[20] Section 2(3), 4(a), and 5 of the IG Act; Section 103H(k) of the Nat'l Sec. Act; Section 17(d) of the CIA Act. The Inspector General of the Department of Justice makes its publicly released reports available on the internet at http://oig.justice.gov/reports/all.htm. Similarly, the Inspector General for the Intelligence Community makes it semi-annual reports publicly available at https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig.
[21] Section 7 of the IG Act; Section 103H(g)(3) of the Nat'l Sec. Act; Section 17(e)(3) of the CIA Act.

Branch influences increases the effectiveness of IG oversight. Because of this independence, IGs can promote economy, efficiency, and accountability in Executive Branch agencies with objectivity and integrity.

Finally, Congress has established the Council of Inspectors General on Integrity and Efficiency. This Council, among other things, develops IG standards for audits, investigations and reviews; promotes training; and has the authority to conduct reviews of allegations of IG misconduct, which serves as a critical eye on IGs, who are entrusted to watch all others. [22]

I hope that this information is helpful to you.

Regards,

Robert S. Litt
General Counsel

[22] Section 11 of the IG Act.

ANNEX VII

Letter from Deputy Assistant Attorney General and Counselor for International Affairs Bruce Swartz, U.S. Department of Justice

February 19, 2016

Mr. Justin S. Antonipillai
Counselor
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, DC 20230

Mr. Ted Dean
Deputy Assistant Secretary
International Trade Administration
1401 Constitution Ave., NW
Washington, DC 20230

Dear Mr. Antonipillai and Mr. Dean:

This letter provides a brief overview of the primary investigative tools used to obtain commercial data and other record information from corporations in the United States for criminal law enforcement or public interest (civil and regulatory) purposes, including the access limitations set forth in those authorities.[1] These legal processes are nondiscriminatory in that they are used to obtain information from corporations in the United States, including from companies that will self-certify through the US/EU Privacy Shield framework, without regard to the nationality of the data subject. Further, corporations that receive legal process in the United States may challenge it in court as discussed below.[2]

Of particular note with respect to the seizure of data by public authorities is the Fourth Amendment to the United States Constitution, which provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and

[1] This overview does not describe the national security investigative tools used by law enforcement in terrorism and other national security investigations, including National Security Letters (NSLs) for certain record information in credit reports, financial records, and electronic subscriber and transaction records, *see* 12 U.S.C. § 3414; 15 U.S.C. § 1681u; 15 U.S.C. § 1681v; 18 U.S.C. § 2709, and for electronic surveillance, search warrants, business records, and other collection of communications pursuant to the Foreign Intelligence Surveillance Act, *see* 50 U.S.C. § 1801 *et seq*.

[2] This paper discusses federal law enforcement and regulatory authorities; violations of state law are investigated by states and are tried in state courts. State law enforcement authorities use warrants and subpoenas issued under state law in essentially the same manner as described herein, but with the possibility that state legal process may be subject to protections provided by State constitutions that exceed those of the U.S. Constitution. State law protections must be at least equal to those of the U.S. Constitution, including but not limited to the Fourth Amendment.

seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. As the United States Supreme Court stated in *Berger v. State of New York*, "[t]he basic purpose of this Amendment, as recognized in countless decisions of this Court, is to safeguard the privacy and security of individuals against arbitrary invasions by government officials." 388 U.S. 41, 53 (1967) (*citing Camara v. Mun. Court of San Francisco*, 387 U.S. 523, 528 (1967)). In domestic criminal investigations, the Fourth Amendment generally requires law enforcement officers to obtain a court-issued warrant before conducting a search. *See Katz v. United States*, 389 U.S. 347, 357 (1967). When the warrant requirement does not apply, government activity is subject to a "reasonableness" test under the Fourth Amendment. The Constitution itself, therefore, ensures that the U.S. government does not have limitless, or arbitrary, power to seize private information.

Criminal Law Enforcement Authorities:

Federal prosecutors, who are officials of the Department of Justice (DOJ), and federal investigative agents including agents of the Federal Bureau of Investigation (FBI), a law enforcement agency within DOJ, are able to compel production of documents and other record information from corporations in the United States for criminal investigative purposes through several types of compulsory legal processes, including grand jury subpoenas, administrative subpoenas and search warrants, and may acquire other communications pursuant to federal criminal wiretap and pen register authorities.

Grand Jury or Trial Subpoenas: Criminal subpoenas are used to support targeted law enforcement investigations. A grand jury subpoena is an official request issued from a grand jury (usually at the request of a federal prosecutor) to support a grand jury investigation into a particular suspected violation of criminal law. Grand juries are an investigative arm of the court and are impaneled by a judge or magistrate. A subpoena may require someone to testify at a proceeding, or to produce or make available business records, electronically stored information, or other tangible items. The information must be relevant to the investigation and the subpoena cannot be unreasonable because it is overbroad, or because it is oppressive or burdensome. A recipient can file a motion to challenge a subpoena based on those grounds. *See* Fed. R. Crim. P. 17. In limited circumstances, trial subpoenas for documents may be used after the case has been indicted by the grand jury.

Administrative Subpoena Authority: Administrative subpoena authorities may be exercised in criminal or civil investigations. In the criminal law enforcement context, several federal statutes authorize the use of administrative subpoenas to produce or make available business records, electronically stored information, or other tangible items in investigations involving health care fraud, child abuse, Secret Service protection, controlled substance cases, and Inspector General investigations implicating government agencies. If the government seeks to enforce an administrative subpoena in court, the recipient of the administrative subpoena, like the recipient of a grand jury subpoena, can argue that the subpoena is unreasonable because it is overbroad, or because it is oppressive or burdensome.

Court Orders For Pen Register and Trap and Traces: Under criminal pen register and trap and trace provisions, law enforcement may obtain a court order to acquire real-time, non-content dialing, routing, addressing and signaling information about a phone number or email

upon certification that the information provided is relevant to a pending criminal investigation. *See* 18 U.S.C. §§ 3121-3127. The use or installation of such a device outside the law is a federal crime.

Electronic Communications Privacy Act (ECPA): Additional rules govern the government's access to subscriber information, traffic data and stored content of communications held by ISPs telephone companies, and other third party service providers, pursuant to Title II of ECPA, also called the Stored Communications Act (SCA), 18 U.S.C. §§ 2701–2712. The SCA sets forth a system of statutory privacy rights that limit law enforcement access to data beyond what is required under constitutional law from customers and subscribers of Internet service providers. The SCA provides for increasing levels of privacy protections depending on the intrusiveness of the collection. For subscriber registration information, IP addresses and associated time stamps, and billing information, criminal law enforcement authorities must obtain a subpoena. For most other stored, non-content information, such as email headers without the subject line, law enforcement must present specific facts to a judge demonstrating that the requested information is relevant and material to an ongoing criminal investigation. To obtain the stored content of electronic communications, generally, criminal law enforcement authorities obtain a warrant from a judge based on probable cause to believe the account in question contains evidence of a crime. The SCA also provides for civil liability and criminal penalties.

Court Orders for Surveillance Pursuant to Federal Wiretap Law: Additionally, law enforcement may intercept in real time wire, oral or electronic communications for criminal investigative purposes pursuant to the federal wiretap law. *See* 18 U.S.C. §§ 2510-2522. This authority is available only pursuant to a court order in which a judge finds, *inter alia*, that there is probable cause to believe that the wiretap or electronic interception will produce evidence of a federal crime, or the whereabouts of a fugitive fleeing from prosecution. The statute provides for civil liability and criminal penalties for violations of the wiretapping provisions.

Search Warrant – Rule 41: Law enforcement can physically search premises in the United States when authorized to do so by a judge. Law enforcement must demonstrate to the judge based on a showing of "probable cause" that a crime was committed or is about to be committed and that items connected to the crime are likely to be found in the place specified by the warrant. This authority is often used when a physical search by police of a premise is needed due to the danger that evidence may be destroyed if a subpoena or other production order is served on the corporation. *See* U.S. Const. amend. IV (discussed in further detail above), Fed. R. Crim. P. 41. The subject of a search warrant may move to quash the warrant as overbroad, vexatious or otherwise improperly obtained and aggrieved parties with standing may move to suppress any evidence obtained in an unlawful search. *See Mapp v. Ohio*, 367 U.S. 643 (1961).

DOJ Guidelines and Policies: In addition to these Constitutional, statutory and rule-based limitations on government access to data, the Attorney General has issued guidelines that place further limits on law enforcement access to data, and that also contain privacy and civil liberty protections. For instance, the Attorney General's Guidelines for Domestic Federal Bureau of Investigation (FBI) Operations (September 2008) (hereinafter AG FBI Guidelines), available at http://www.justice.gov/archive/opa/docs/guidelines.pdf, set limits on use of investigative means to seek information related to investigations that involve federal crimes. These guidelines require that the FBI use the least intrusive investigative methods

feasible, taking into account the effect on privacy and civil liberties and the potential damage to reputation. Further, they note that "it is axiomatic that the FBI must conduct its investigations and other activities in a lawful and reasonable manner that respects liberty and privacy and avoids unnecessary intrusions into the lives of law-abiding people." *See* AG FBI Guidelines at 5. The FBI has implemented these guidelines through the FBI Domestic Investigations and Operations Guide (DIOG), available at https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20(DIOG), a comprehensive manual that includes detailed limits on use of investigative tools and guidance to assure that civil liberties and privacy are protected in every investigation. Additional rules and policies that prescribe limitations on the investigative activities of federal prosecutors are set out in the **United States Attorneys' Manual** (USAM), also available online at http://www.justice.gov/usam/united-states-attorneys-manual.

Civil and Regulatory Authorities (Public Interest):

There are also significant limits on civil or regulatory (*i.e.*, "public interest") access to data held by corporations in the United States. Agencies with civil and regulatory responsibilities may issue subpoenas to corporations for business records, electronically stored information, or other tangible items. These agencies are limited in their exercise of administrative or civil subpoena authority not only by their organic statutes, but also by independent judicial review of subpoenas prior to potential judicial enforcement. *See, e.g.*, Fed. R. Civ. P. 45. Agencies may seek access only to data that is relevant to matters within their scope of authority to regulate. Further, a recipient of an administrative subpoena may challenge the enforcement of that subpoena in court by presenting evidence that the agency has not acted in accordance with basic standards of reasonableness, as discussed earlier.

There are other legal bases for companies to challenge data requests from administrative agencies based on their specific industries and the types of data they possess. For example, financial institutions can challenge administrative subpoenas seeking certain types of information as violations of the Bank Secrecy Act and its implementing regulations. *See* 31 U.S.C. § 5318, 31 C.F.R. Part X. Other businesses can rely on the Fair Credit Reporting Act, *see* 15 U.S.C. § 1681b, or a host of other sector specific laws. Misuse of an agency's subpoena authority can result in agency liability, or personal liability for agency officers. *See, e.g.*, Right to Financial Privacy Act, 12 U.S.C. §§ 3401–3422. Courts in the United States thus stand as the guardians against improper regulatory requests and provide independent oversight of federal agency actions.

Finally, any statutory power that administrative authorities have to physically seize records from a company in the United States pursuant to an administrative search must meet the requirements of the Fourth Amendment. *See See v. City of Seattle*, 387 U.S. 541 (1967).

Conclusion

All law enforcement and regulatory activities in the United States must conform to applicable law, including the U.S. Constitution, statutes, rules, and regulations. Such activities must also comply with applicable policies, including any Attorney General Guidelines governing federal law enforcement activities. The legal framework described above limits the ability of U.S. law enforcement and regulatory agencies to acquire information from corporations in the United States -- whether the information concerns U.S. persons or citizens of foreign countries --and in addition permits judicial review of any government requests for data pursuant to these authorities.

Sincerely,

_____

Bruce C. Swartz
Deputy Assistant Attorney General and
Counselor for International Affairs