EUROPEAN
COMMISSION

Brussels, 18.10.2017
SWD(2017) 344 final

COMMISSION STAFF WORKING DOCUMENT
Accompanying the document

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the first annual review of the functioning of the EU–U.S. Privacy Shield

{COM(2017) 611 final}

1. INTRODUCTION

This document presents the findings of the Commission services on the implementation and enforcement of the EU-U.S. Privacy Shield framework (the "Privacy Shield") in its first year of operation. The findings are based on information gathered from relevant stakeholders and the U.S. authorities both in the preparation of and during the Annual Joint Review meetings held in Washington, D.C., on 18 and 19 September 2017. The findings have further been informed by publicly available material, such as court decisions, implementing rules and procedures of relevant U.S. authorities, reports and studies from non-governmental organisations, transparency reports issued by Privacy Shield-certified companies, as well as media reports. The eight representatives designated by the Article 29 Working Party[1] (the "WP29") to participate to the Annual Joint Review, together with the Commission, have been consulted on this document and provided feedback on the factual findings.[2]

2. THE EU-U.S. PRIVACY SHIELD FRAMEWORK

In its Decision of 12 July 2016[3] (the "adequacy decision"), the Commission concluded that the United States ensures an adequate level of protection for personal data transferred from the European Union to U.S. companies certified under the Privacy Shield. As a consequence, such data transfers are permitted under EU data protection law without additional requirements.[4]

The Privacy Shield is a framework for the transfer of personal data from the EU to companies in the U.S. for commercial purposes. It is based on a certification system by which U.S. companies commit to adhere to a set of privacy principles – the EU-U.S. Privacy Shield framework Principles[5] (hereinafter also referred to as: "the Principles"). While certification is voluntary, companies that have been certified are obliged to comply with the Principles, as they become enforceable under U.S. law.[6] The Privacy Shield framework is administered and monitored by the U.S. Department of Commerce (DoC) and compliance with the Principles is enforced by the Federal Trade Commission (FTC) or the Department of Transportation

[1] The Article 29 Working Party is the advisory body that brings together the national authorities of the Member States as well as the European Data Protection Supervisor.

[2] See also Article 29 Working Party Press Release "First annual Joint Review of the Privacy Shield" available at http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 (under "Letters, Opinions and other documents").

[3] Article 1(1) of Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 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, OJ L 207, 1.8.2016, p.1.

[4] Pursuant to Article 25(1) of Directive 95/46/EC, Member States are required to provide that the transfer of personal data to a third country may take place only if, without prejudice to compliance with the national rules adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

[5] Annex II to the adequacy decision.

[6] See recital 54 and Annex II. Failure to comply with the Principles is enforceable under Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive acts in or affecting commerce.

(DoT), depending on which authority has jurisdiction over the Privacy Shield-certified company.

The Privacy Shield reflects the principles and requirements laid down by the European Court of Justice in its judgment in the *Schrems* case,[7] which invalidated the previous Safe Harbour framework. It provides for a number of novel elements, compared to the Safe Harbour, which enhance the protection of personal data when transferred to the United States. This includes stricter obligations on Privacy Shield-certified companies, for example regarding limitations on how long a company may retain personal data or the conditions under which data can be shared with third parties outside the framework (so-called "onward transfers"). It also provides for more regular and rigorous monitoring by the DoC and significantly strengthens the possibilities for EU individuals to obtain redress. In addition, the Privacy Shield builds on specific written representations and assurances made by the U.S. government that access by public authorities for national security, law enforcement and other public interest purposes to personal data transferred under the Privacy Shield is subject to clear limitations and safeguards. To this end, it also creates an entirely new redress mechanism, the Ombudsperson.

3. THE FIRST ANNUAL REVIEW – BACKGROUND, PREPARATION AND CONSULTATION OF STAKEHOLDERS

To regularly verify that the findings in the Commission's adequacy decision are still factually and legally justified, the Privacy Shield framework provides for an annual evaluation on the basis of all the available information, including the information received as part of the Annual Joint Review.[8]

The Commission conducts the annual review together with the U.S. authorities, covering all aspects of the Privacy Shield, both the "commercial" side (compliance by companies and related oversight and enforcement), as well as aspects relating to government access to personal data. The annual review is open to the participation of representatives of the WP29.[9]

The Privacy Shield framework has been operational since 1 August 2016. Taking into account that this is the first year of its operation, the Commission's annual review has thus focused on verifying that all the mechanisms and procedures provided for in the framework – many of which were newly created – have been fully implemented and are functioning in the way that is foreseen in the adequacy decision. Moreover, the Commission has put particular emphasis on checking whether and how the various U.S. authorities involved in the implementation of the framework have lived up to their commitments, both as regards the administration and supervision of the commercial aspects of the Privacy Shield, and with respect to government access to personal data. The change of the U.S. administration in January 2017 made this particularly relevant.

---

7 Judgment of the Court of Justice of the European Union of 6 October 2015 in Case C-362/14, *Maximilian Schrems v Data Protection Commissioner* ("*Schrems*").

8 Recitals 145-149 and Article 4(4) of the adequacy decision.

9 Recitals 146 and 147 of the adequacy decision.

In order to prepare the annual review, the Commission services gathered information and feedback on the implementation and functioning of the Privacy Shield framework from a wide range of relevant stakeholders.

On 2 June 2017, the Commission services sent questionnaires to nine trade associations in the U.S.[10] with a view to collecting input from those of their members that are Privacy Shield-certified. Among others, these questionnaires covered various aspects relating to the compliance of companies with their Privacy Shield-obligations, including the policies developed by these companies to ensure the respect of such obligations (compliance programs, training etc.), the application in practice of certain privacy principles (e.g. the "accountability for onward transfers" principle) as well as specific issues such as automated decision-making.[11]

On the same day, the Commission services also sent questionnaires to eight Non-Governmental Organisations (NGOs) which are active in the field of fundamental rights and in particular digital rights and privacy.[12] Again, these questionnaires covered aspects relating to company compliance, but also government access, the functioning of redress mechanisms and relevant developments in the U.S. legal system.

The Commission services received written replies to its questionnaires from trade associations and NGOs at the beginning of July 2017.

Moreover, based also on input received from the WP29, the Commission services sent a detailed set of questions to the U.S. authorities that administer and oversee the Privacy Shield framework. At the beginning of September 2017, the Commission services received a first reply and a set of documents from the U.S. authorities, which was complemented by additional information and further documents in the run-up to and at the Annual Joint Review.

After having analysed the input received, the Commission services met with the representatives of the WP29 (on 24 August, 8 September and 17 September 2017) in order to further prepare the Annual Joint Review and discuss which aspects require additional information-gathering and clarification.

Throughout the preparatory phase, the Commission services had exchanges with trade associations, individual companies and NGOs to follow-up on the input provided. This notably included a meeting on 8 September 2017 with representatives of the NGOs that had answered to the Commission's questionnaire, to further discuss their replies.

---

[10] Namely, Software & Information Industry Association (SIIA), U.S. Chamber of Commerce, Information Technology Industry Council (ITI), The Software Alliance (BSA), Centre for Information Policy Leadership (CIPL), Internet Association, Interactive Advertising Bureau (IAB), United States Council for International Business (USCIB), and Computer & Communications Industry Association (CCIA).

[11] The Commission's adequacy decision (recital 25) sets out that automated decision-making, including an exchange on the similarities and differences in the EU and U.S. approach in this regard, will be part of the first annual review as well as of subsequent reviews as appropriate.

[12] Namely, Human Rights Watch, American Civil Liberties Union, Consumer Federation of America, Center for Digital Democracy, New America's Open Technology Institute, Access Now, Electronic Frontier Foundation (EFF) and Electronic Privacy Information Center (EPIC).

The Commission also exchanged views on the Privacy Shield and the first annual review with Members of the European Parliament, in particular those who had participated in the LIBE Committee's visit to Washington, D.C., in July 2017, which focused *inter alia* on the state of privacy protection in the United States.

The Commission also presented its approach to the annual review to Member States and received their feedback in that respect, notably in meetings of the Council Working Party on Information Exchange and Data Protection ("DAPIX") in June-September 2017. Member States were also kept informed at the meetings of the Transatlantic Relations ("COTRA") group.

4. THE FIRST ANNUAL REVIEW – PROCESS AND FINDINGS

The first Annual Joint Review took place in Washington, D.C., on 18-19 September 2017. On the U.S. side, representatives of the DoC, the FTC, the DoT, the Department of State, the Office of the Director of National Intelligence (ODNI) and the Department of Justice (DoJ) participated in the review, as well as the acting Ombudsperson, a Member of the Privacy and Civil Liberties Oversight Board (PCLOB) and the General Counsel of the Office of the Inspector General of the Intelligence Community.

Moreover, representatives of organisations that provide independent dispute resolution under the Privacy Shield, the American Arbitration Association and Privacy Shield-certified companies[13] provided information during the relevant review sessions.

The Annual Joint Review was opened by Commissioner for Justice, Consumers and Gender Equality, Věra Jourová, U.S. Secretary of Commerce Wilbur Ross and FTC Acting Chairman Maureen Olhausen. It was conducted for the EU by representatives of the European Commission's Directorate General for Justice and Consumers. The EU delegation also included eight representatives designated by the WP29.[14]

The review was organised by topics, with each dedicated agenda point introduced by a short presentation by the relevant U.S. authority or organisation followed by a detailed question-and-answer session. It covered the "commercial" aspects of the framework on the first day and issues relating to government access to personal data on the second day.

4.1. COMMERCIAL ASPECTS

With regard to the commercial aspects, the Commission focused its review on the actions that the relevant U.S. authorities, in particular DoC and FTC, have taken in the past year to comply with their commitments regarding the administration, supervision and enforcement of

[13] Namely, Cisco, Microsoft, Ernst & Young, and Hunton &Williams, a law firm that advises many companies certifying under the Privacy Shield.

[14] See Letter from the WP29 to Commissioner Jourová of 15 June 2017. The text of the letter is available at http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083, under "Letters, Opinions and other documents".

the Privacy Shield framework. In addition, the Commission has assessed whether complaints have been lodged by EU individuals and handled effectively, *inter alia* through the Independent Recourse Mechanisms. Furthermore, the Commission enquired about the specific topic of automated decision-making and developments in U.S. law which have taken place since the adoption of the adequacy decision and could be relevant for the functioning of the commercial aspects of the Privacy Shield.

4.1.1. The certification process

In order to be able to receive personal data transferred from the EU on the basis of the Privacy Shield, a company must certify, and subsequently re-certify on an annual basis, with the DoC its adherence to the Principles. The certification requires that a company is subject to the investigatory and enforcement powers of the FTC or the DoT, publicly declares its commitment to comply with the Principles, publicly discloses its privacy policy and fully implements the Principles.[15] Prior to finalising a certification, the DoC verifies whether the company has met all certification requirements.[16]

At the date of the review meeting, over 2,400 companies had certified under the Privacy Shield framework and around 400 applications for certification were under review by the DoC.[17] These numbers reflect that adherence to the framework is significant, also when compared to the Safe Harbour: after only one year of operation, more companies are certified under the Privacy Shield framework than were certified under the Safe Harbour after the first ten years of its existence.[18] Moreover, the number of Privacy Shield-certified companies continues to grow steadily. According to the DoC, approximately 20 new companies apply for certification each week. Participation in the program includes both companies headquartered in the U.S. and (currently) more than 100 EU-based companies with respect to their subsidiaries in the U.S.

To administer the certification process, the DoC has developed and put in place the necessary tools and procedures for handling application requests by companies. Companies submit their applications for certification, including the relevant documentation, via the DoC's Privacy Shield website (https://www.privacyshield.gov/PrivacyShield/ApplyNow). In each section of the web form that companies have to complete, the DoC provides information on the company's respective obligations under the Privacy Shield. As regards annual re-certifications, the DoC has established a process according to which the DoC sends companies an e-mail reminder (indicating that the annual re-certification is due) one month prior to the anniversary of the initial certification date, and again two weeks and then one day prior to that date. The process for reviewing applications for re-certification is identical to the review process used for the initial certification. A team of ten DoC staff members reviews the applications for certification, with each application being assigned to a specific staff member who remains responsible for the relevant company throughout the certification process.

[15] Annex II to the adequacy decision, para. 2.
[16] Annex I (Annex 1) to the adequacy decision, p. 3.
[17] Ten companies did not complete the certification process but withdrew before finalisation of the certification.
[18] In 2010, there were 512 first-time certifications and 1,417 re-certifications for the Safe Harbour.

It results from the annual review that, prior to finalising a certification, the DoC checks the information provided in a company's application, assesses if there are deficiencies and, if deficiencies are found, requests the company concerned to address them. This request then triggers a process of consultation between the DoC and the company concerned[19] during which the DoC has often provided further explanations on certain aspects of the certification requirements, and the company is typically asked to provide additional information, clarify the information submitted and/or make amendments to its privacy policy. The DoC has reported that for the majority of certifications so far, such follow-up has been necessary. The business representatives present during the Annual Joint Review have confirmed that a number of exchanges with the DoC were needed before their certifications could be finalised.

Consultations have taken place for example with respect to companies' descriptions of the purposes of data processing, which the DoC in many cases has considered to be insufficient and too vague. The DoC has then followed up with the respective company to determine and correctly describe the specific purposes for which it uses the data received from the EU under the Privacy Shield. Also, an incorrect determination of the entities and subsidiaries that a company intends to cover with its application for certification has regularly triggered the consultation process. On the one hand, companies have described these entities in a too general manner (with indications such as "all U.S. subsidiaries") that would not allow individuals to determine which entity is covered by the certification and which is not. On the other hand, companies have indicated that non-U.S. entities and subsidiaries are covered by the certification, although only companies which are based in the U.S. can adhere to the Privacy Shield framework.[20]

Moreover, the DoC reported that it does not only rely on the information provided by the company, but also carries out cross-checks with other relevant authorities and bodies in order to verify the accuracy of such information. For instance, when reviewing an application for certification, the DoC assesses whether the applicant has identified the correct enforcement authority with respect to the company's activities covered by the application, and systematically consults with the relevant enforcement authority in case of doubt.[21]

---

[19] It also triggers a 45-day deadline within which the company is required to finalise its certification (see further down in the text).

[20] To address these issues, the DoC issued two additional FAQs available on the Privacy Shield website: one that clarifies that companies can either list the entities and subsidiaries by name, or by indicating "all U.S. subsidiaries using brand name [X]", excluding particular entities, if applicable; and one that clarifies that only U.S. entities and subsidiaries can qualify as covered entities.

[21] A company may only certify if it is subject to the investigatory and enforcement powers of the FTC or the DoT. The FTC and DoT's respective jurisdictions are described on the Privacy Shield website as follows: "*Generally, the FTC's jurisdiction covers acts or practices in or affecting commerce by any "person, partnership, or corporation." The FTC does not have jurisdiction over most depository institutions (banks, federal credit unions, and savings & loan institutions), telecommunications and interstate transportation common carrier activities, air carriers, labor associations, most non-profit organisations, and most packer and stockyard activities. In addition, the FTC's jurisdiction with regard to insurance activities is limited to certain circumstances. Note that to be transferred in reliance on the Privacy Shield, personal data must be processed in connection with an activity that is subject to the jurisdiction of at least one appropriate statutory body listed in the Framework. The DOT has exclusive jurisdiction over U.S. and foreign air carriers. The DOT and the FTC share jurisdiction over ticket agents that market air transportation. If you*

In addition, in order to verify whether a company that applies for certification has indeed registered with an independent recourse mechanism, the DoC has developed a method of verifying registration with the respective independent recourse mechanism. If a company uses EU Data Protection Authorities (DPAs) as independent recourse mechanism, the U.S. Council for International Business transmits the receipt indicating payment of the DPA fee to the DoC, so that the latter is able to verify that the payment has been made.

Finally, the DoC explained that improvements have been made to the process in light of issues that emerged during the first year of operation of the Privacy Shield with respect to the certification process and requirements. In particular, as regards the certification process, the DoC noticed in the course of the year that some companies initiated the process by submitting their application for certification via the online tool, but then, when requested by the DoC to provide further information, clarify certain aspects of their submission or correct deficiencies, did not react to that, so that the DoC was not able to finalise the certification. As a consequence, the concerned certifications remained pending: the companies could not be included in the DoC's list of Privacy Shield-certified companies, while at the same time the companies' privacy policy already contained a reference to the Privacy Shield. To address this issue, the DoC introduced a 45-day deadline (starting from the day on which the DoC raises issues in the context of the review process) within which companies have to complete their certification, including by taking the follow-up actions required by the DoC. Upon expiry of the deadline, and in case the concerned company would have failed to take such actions, the DoC considers its application for certification as withdrawn. The DoC then informs the company that it must remove public references to the Privacy Shield or it will otherwise be referred to the FTC.

The Commission services welcome the introduction of a 45-day deadline for completion of the certification process as a relevant first step that improves the efficiency of the process and better ensures legal certainty for all parties involved.

However, further improvements of the procedure should be introduced, as it results from the annual review that companies can make public representations about their Privacy Shield certification while the certification process is not yet completed, for example because the DoC has follow-up questions or has identified deficiencies that need to be corrected. Consequently, there may be a discrepancy between information that is publicly available, e.g. a company's privacy policy, and the DoC's Privacy Shield list which includes a company only once the certification is finalised. To ensure legal certainty and avoid "false claims", it is important that companies are not allowed to publicly refer to their adherence to the framework before the DoC has finalised the certification and included the company in the Privacy Shield list. This should not create any difficulty for the certification process, as companies can, when submitting their application, provide the DoC with a link to their privacy policy (including the

---

are uncertain as to whether your organisation falls under the jurisdiction of either the FTC or DOT, then please be sure to contact the Privacy Shield Team at the Department of Commerce for more information". No airline company had certified under the Privacy Shield at the time of the Annual Joint Review.

Privacy Shield reference) which only becomes accessible by the public once the certification is finalised.

With respect to the certification requirements, the DoC reports that it became aware of two issues, one concerning the jurisdiction of the relevant enforcement authority, the other one concerning the identification of entities covered by the Privacy Shield certification.

First, as regards jurisdiction, the DoC noted that in their application a number of companies indicated the DoT as the competent enforcement authority, which, considering the limited scope of DoT jurisdiction,[22] appeared incorrect. Further checks revealed that most of these companies had indeed indicated the wrong enforcement authority.[23] As a consequence, the DoC introduced systematic checks to verify the accuracy of the designation of the competent enforcement authority, including through cooperation with the FTC and DoT (as already described above).

Second, when the DoC noted that companies named the entities to be covered by the certification in a too general manner or listed entities which by definition could not be covered by the Privacy Shield framework, it contacted the companies concerned. It also also amended existing and issued further guidance on the subject of covered entities on its website, aimed at avoiding such problems in the future.

The way in which the DoC administers the certification process appears satisfactory. The Department should continue to closely oversee the proper functioning of the process and effectively control the accuracy and completeness of the information provided by companies as part of their request for certification and re-certification.

4.1.2. Monitoring and supervision of Privacy Shield-certified companies

After companies have certified to the Privacy Shield framework, the DoC continues to monitor and supervise compliance with the Principles throughout the companies' adherence to the framework. More specifically, the DoC has committed to strengthen supervision by, *inter alia*, conducting periodic *ex officio* compliance reviews, including through sending detailed questionnaires, and by searching for and addressing false claims.[24]

The Commission services note that during the first year of operation of the Privacy Shield, the DoC's efforts have been focused more on certification than on monitoring and supervision. The DoC put in place the infrastructure and procedures for managing the new certification process under the Privacy Shield, and has worked on their improvement to address issues that arose in the course of the year as companies were joining the system. Moreover, it had to

[22] See above, footnote 21.

[23] Initially, 27 companies indicated DoT as their regulator (some of them mistakenly). According to information received by the DoC further to the Annual Joint Review, as of 21 September 2017, 13 companies on the Privacy Shield List have indicated in their Privacy Shield records that they are subject to DoT jurisdiction. The DoC has confirmed with 10 companies that they are subject to DoT jurisdiction, while the assessment is still ongoing with respect to the remaining 3.

[24] See Annex I (Annex 1) to the adequacy decision.

review a large number of applications for certification, in particular in the first months after the adoption of the Commission's adequacy decision.

The Commission services note and welcome that the DoC has also developed instruments intended to ensure an effective supervision of compliance by certified companies. In particular, it has drawn up questionnaires to be sent to certified companies in various situations, namely for compliance review, in case a company voluntarily withdraws from the Privacy Shield, fails to complete the annual re-certification or is found to persistently fail to comply with the Principles.[25] The Compliance Review Questionnaire is an important tool to be used by the DoC to monitor on an ongoing basis effective compliance with the framework. Such compliance reviews have to take place in particular when the DoC receives a credible complaint or otherwise becomes aware that a company may not be in compliance with the Principles. Companies are obliged to respond to the questionnaires within 30 days, while failure to do so may trigger enforcement action by the relevant enforcement authority (at the time of the Annual Joint Review, these Compliance Review Questionnaires had not been used yet).

Furthermore, the DoC has created, in consultation with the WP29, a standard referral form to be used by DPAs in case a DPA believes that a company is not complying with the Principles. The standard referral form is aimed at facilitating the referral of such a company to the DoC for further compliance review.

In terms of concrete actions taken by the DoC to ensure compliance with the Principles, the Commission services note that the DoC in June 2017 reminded all Privacy Shield companies that had certified within the first two months of the framework's operation of the nine-month deadline to bring existing commercial relationships with third parties into conformity with the Accountability for Onward Transfers Principle. With respect to compliance with the same principle, the DoC also responded to inquiries received from companies, for example as to the applicable deadline and the contractual requirements. The DoC also proactively contacted major cloud service providers to inform them about the requirements and address questions. However, the DoC has not made use of the possibility provided in the Privacy Shield to request copies of the contractual terms used by certified companies in their contracts with third parties to ensure compliance with the Principle.[26]

The DoC has also established a system according to which it verifies on a monthly basis the continued accessibility of the links to the privacy policies of certified companies which are displayed on the DoC's Privacy Shield list. This exercise is conducted by using a program

[25] If companies voluntarily withdraw from the Privacy Shield or fail to re-certify, the DoC has the obligation to follow-up with such companies in order to determine how they treat the personal data they have received from the EU while participating in the Privacy Shield. A company may choose to delete or return this data, or otherwise must continue to process it in accordance with the Principles or by providing adequate protection for the data by another authorised means and affirm to the DoC on an annual basis its commitment to do so. In case of persistent failure to comply with the Principles, a company is not entitled to retain any personal data that it has received under the Privacy Shield, which is again to be verified by the DoC. See Annex I (Annex 1) to the adequacy decision.

[26] Annex II to the adequacy decision, Section II.3.b.

that automatically identifies erroneous links. If a link is inaccessible, the DoC contacts the relevant company and updates the link on its Privacy Shield list accordingly.

Moreover, the DoC has referred 11 companies to the FTC on the basis of false claims of participation in the Privacy Shield framework. These cases were detected by the DoC because the companies had applied for certification under the Privacy Shield but had failed to complete their certification within the newly set 45-day deadline and had not removed references to the Privacy Shield in their privacy policies. As explained below, three of these referrals have led to enforcement actions by the FTC.[27] While the Commission services welcome that these cases have been followed-up first by the DoC and subsequently by the FTC (see section 4.1.4 below), they also note that the DoC has not yet conducted active searches for companies' false claims of participation, although under the Privacy Shield the DoC commits to undertake other efforts to identify false claims of Privacy Shield participation, including by conducting internet searches.[28]

Both as regards false claims of participation and compliance reviews more generally, the overall reliability and well-functioning of the Privacy Shield framework requires not only reactive, but also proactive monitoring and supervision by the DoC. Therefore, the DoC should actively search for and address false claims. It should also make use of the tools it has developed over the first year of operation of the Privacy Shield to check, on an ongoing basis, effective compliance of companies with their obligations during the entire "life-cycle" of their adherence to the framework.

4.1.3. Resolution of complaints

An important aspect where the Privacy Shield has brought significant improvements is the effective protection of privacy rights of Europeans. The Privacy Shield provides several alternative[29] redress possibilities: individuals can bring a complaint i) directly to a Privacy Shield-certified company (which now has to respond within a time limit of 45 days), ii) to a free-of-charge independent recourse mechanism ("IRM") designated by the company (such as an Alternative Dispute Resolution Body ("ADR") or the EU DPAs), iii) to the DoC (through national DPAs that will then refer the complaint to the DoC) or iv) directly to the FTC. Moreover, v) if an individual considers that the handling of her/his complaint is not satisfactory, as a 'last resort' mechanism, s/he can have recourse to an arbitration mechanism: the Privacy Shield Panel.[30]

Over the past year, the DPAs on the one hand, and the DoC and FTC, on the other hand, have put in place a number of tools to facilitate cooperation for an effective handling of complaints. Among other things, the DPAs have adopted a standardised complaint form for the

---

[27] As explained during the Annual Joint Review, the FTC did not take action on all of the 11 referrals, as a number of companies completed certification immediately thereafter.

[28] See Annex I (Annex 1) to the adequacy decision.

[29] With the exception of arbitration which is a last resort mechanism, individuals do not have to exhaust all of them or use them in a specific order to obtain redress.

[30] The Commission has issued a guide explaining both the rights and redress possibilities available to individuals in the EU. See http://ec.europa.eu/justice/data-protection/document/citizens-guide_en.pdf.

submission of commercial related complaints, as well as rules of procedure for the "Informal Panel of EU DPAs",[31] the body that provides binding advice to Privacy Shield companies for unresolved complaints. The DoC and the FTC have each identified a "DPA Liaison" to serve as a point of contact for DPAs, *inter alia* to assist with DPAs enquiries regarding a Privacy Shield company's compliance with the Principles. Moreover, the DoC and the FTC have both created standard referral forms (finalised in consultation with the DPAs) to facilitate referrals of companies for further review where a DPA believes that a company is not complying with the Principles.

Based on the information provided by trade associations and companies, and on the feedback received during the Annual Joint Review, it appears that very few complaints have been lodged so far with Privacy Shield companies[32] and IRMs. The FTC received three complaints referring to the Privacy Shield framework during its first year of operation. None came from the EU. The DoC and the DPAs did not receive any complaints.

While a low volume of complaints is perhaps not surprising during the first year of operation of the framework, it may also be indicative of insufficient awareness by individuals. In this respect, the Commission services acknowledge the awareness-raising efforts made by the DoC[33] and the DPAs[34] so far, but intensified actions should be envisaged to better inform individuals about their rights under the framework.

Such communication actions should notably be part of the awareness-raising activities related to the implementation of the EU data protection reform. In this respect, it should be recalled that, under the General Data Protection Regulation[35] (GDPR), controllers will *inter alia* have to inform individuals, where applicable, of the intention to transfer their personal data to a third country that benefits from a Commission adequacy decision.[36] Individuals must

---

[31] Available at http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083, under "Letters, Opinions and other documents".

[32] Among those companies that answered the questionnaire to trade associations, seven have received complaints.

[33] The DoC website provides answers to many frequently asked questions at: www.privacyshield.gov/program-overview. The website includes content tailored to four audiences - U.S. Businesses, EU Businesses, EU Individuals and Data Protection Authorities - to ensure that all stakeholders understand how the framework operates, including specifically in relation to them. Moreover, during the Annual Joint review, the DoC informed the EU delegation that it will carry out a "road show" throughout the U.S. in the coming weeks to present the framework.

[34] Most of the DPAs have published information material on the Privacy Shield, including online complaint forms, on their respective websites. This online material also include documents developed by the WP29 such as "EU-US Privacy Shield - FA Q for European Individuals - wp246" and EU-US Privacy Shield - FAQ for European Businesses - wp245", available at http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083, under "Letters, Opinions and other documents". DPAs have also organised events and conferences to raise awareness.

[35] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016, p. 1.

[36] See Article 13(1)(f) of the GDPR: "*Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information […] (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, […]*".

therefore be informed about the fact that their personal data will be transferred under the safeguards of the Privacy Shield adequacy decision.

Against that background, the handling of complaints will be assessed in more depth in future annual reviews.

4.1.3.1. Complaint handling by companies

The Privacy Shield requires companies to provide recourse for individuals who are affected by non-compliance and thus the possibility for such individuals to lodge complaints and to have these complaints resolved, if necessary, by a decision providing an effective remedy.[37] The company concerned must respond within 45 days of receiving the complaint.

To ensure compliance with their obligations, many of the companies that have responded to the Commission's questionnaire reported that they have put in place dedicated Privacy Shield complaint mechanisms (including, for example, by making available email addresses and online links or webforms where complaints can be made and are regularly monitored, updating internal complaint-handling mechanisms to ensure that complaints are handled within the Privacy Shield 45-day timeline, creating dedicated complaint-handling teams that include personnel from the legal department, and involving the staff of EU-based affiliates to help in complaint-handling and responding to inquiries and requests).[38]

It results from the answers to the questionnaire sent to trade associations that only seven of the respondent Privacy Shield-certified companies reported having received complaints from individuals whose personal data had been transferred under the framework. The companies concerned reported that the complaints received have been handled in an effective manner leading to satisfactory results as no further recourse procedure was triggered. Moreover, it appears that most "complaints" were actually general enquires regarding the Privacy Shield and the company's privacy procedures, which the companies answered within the deadline and with no follow-up from the individuals who had asked the questions. From the feedback received, it also results that some individuals used the complaint mechanism as a means to exercise their rights. The examples reported include questions about the way the respective company complies with the Privacy Shield obligations, requests to provide confirmation that the company participates in the Privacy Shield, data access requests, requests for information on the purpose of collecting the data, requests for information on retention and deletion policies, whether the data will be transferred to another company, and requests to opt out from data sharing with third parties.

---

[37] See recitals 38 *et seq.* and Recourse, Enforcement and Liability Principle in Annex II to the adequacy decision.

[38] To mention a concrete example, one company established a dedicated Privacy Shield enquiry web-form which is directly accessible from the company's Privacy Policy website. The web form is supported by a dedicated team, which reviews and responds to each complaint with the support of the legal team, if necessary. The company also makes a dedicated email alias available on its Privacy Shield certification as an additional contact mechanism. In June 2017, the company in question had received 118 inquiries (102 received via the web form, and 16 received via the dedicated email alias). All the enquiries have been resolved within the 45-day timeline, without further steps being taken by the respective individuals, which seems to indicate that they were satisfied.

4.1.3.2. Complaint handling by independent recourse mechanisms (IRMs)

Individuals can also bring a complaint directly to the independent recourse mechanism (IRM) (either in the United States or in the Union) designated by a company to investigate and resolve individual complaints and to provide appropriate recourse free of charge to the individual.[39]

The company's website must contain the link to the website of the designated IRM[40] and provide further information, including the procedures to follow for lodging complaints.

A Privacy Shield-certified company is free to opt for an EU DPA to act as its IRM. At the date of the annual review, 455[41] companies have done so, including several large companies such as Google and Microsoft. Moreover, when Privacy Shield-certified companies handle human resources (personnel) data, submission to DPA oversight is mandatory.[42] This means that, as an employee, an individual can always address her/his complaint to her/his local DPA with respect to employment-related data transferred to a Privacy Shield company.[43]

Over the past year, DPAs have received no complaints, neither as IRM freely chosen by a company nor as a consequence of the companies' processing of human resources data.

As noted above, to comply with its obligation to verify companies' registrations with IRMs,[44] the DoC has worked with each IRM to develop a method of verifying that companies have indeed registered with the IRM indicated in their certification. The DoC also verifies that each company using DPAs as an IRM has paid the required fee by confirming that the receipt has been received. The DoC has put in place a system to ensure that no certification will be finalised before it ascertains that a company has registered with the identified IRM or paid the DPA fee, where the DPA fee is due.

---

39 See recital 45 and Recourse, Enforcement and Liability Principle in Annex II to the adequacy decision. Sanctions and remedies imposed by such a body must be sufficiently rigorous to ensure compliance by companies with the Principles and should provide for a reversal or correction by the company of the effects of non-compliance and, depending on the circumstances, the termination of the further processing of the personal data at stake and/or their deletion, as well as publicity for findings of non-compliance. Independent recourse mechanisms designated by a company will be required to include on their public websites relevant information regarding the Privacy Shield and the services they provide under the framework.

40 BBB (702), TRUSTe (521) and JAMS (458) are the IRMs most frequently selected. They are followed by EU DPAs, ICDR/AAA, DMA, Privacy Trust, Insights Association, VeraSafe and Whistic.

41 223 companies use DPAs for both HR and non-HR data; 232 companies use DPAs for non-HR data only.

42 See recital 40 of the adequacy decision and Annex II, p. 54 *in fine*.

43 The complaint received by a DPA will then be assessed by an informal panel of DPAs (composed of one lead and two co-reviewer DPAs) that will deliver its advice to the organisation within 60 days of receiving the complaint. The individual concerned will be informed about that advice, which will be made public to the extent possible. The company concerned has 25 days then to comply, failing which the DPA may refer the case to the FTC for possible enforcement action. It may also inform the DoC about the company's refusal to comply with the DPA's advice, which may lead to the removal of the company from the Privacy Shield List, if the company persists in its non-compliance.

44 Annex I (Annex 1) to the adequacy decision.

All IRMs are required to publish an annual report providing aggregate statistics regarding their services.[45] Reports by all concerned organisations had been issued by the time of the Annual Joint Review.

The published reports show that a very small number of Privacy Shield-related complaints have been handled by IRMs throughout this first year of operation of the Privacy Shield framework.

More specifically, Better Business Bureau (BBB) received 180 complaints, but 179 were determined to be outside the scope of the Privacy Shield program. At the time of the Annual Joint Review, one complaint was still under review for admissibility. Similarly, TRUSTe received 788 complaints, but only one proved to be about compliance with the Principles (and required issue-specific changes by the company concerned, such as to unsubscribe the user and to close the account), while four were pending resolution as of the close of the reporting period.[46] DMA received 14 inquiries, two of which qualified under the Privacy Shield framework (one objection to receiving online ads and one request to be removed from an emailing list). The few complaints received over the past year have all been resolved in a satisfactory manner. The other reports published by the IRMs indicate that no Privacy Shield-related complaint was received during the reporting period.

The Commission services note that the way in which the reports by IRMs present aggregate statistics regarding their dispute resolution services varies significantly (as also acknowledged by the DoC during the Annual Joint Review). The format of the reports should be standardised in the future, so as to allow a clear comparative reading.

4.1.3.3. Complaint handling by the DoC and by the FTC

Individuals can also address complaints to their home country DPA, for it to refer the complaint to the DoC. To this end, and in compliance with its obligation under the Privacy Shield, the DoC has put in place a dedicated contact (a "DPA Liaison") that is responsible for liaising directly with DPAs. In addition, to facilitate the submission of such complaints, the DoC (in consultation with DPAs) has created a standard referral form for DPAs to submit complaints to the DoC's dedicated contact. The DoC may also forward the complaint to the FTC (or the DoT).[47] No complaints have been channelled to the DoC via the DPAs, over the past year.

---

[45] See recital 45 of the adequacy decision and Annex II, Supplemental Principle 11(d)(iii) (Dispute Resolution and Enforcement).

[46] Approx. 45% of them were closed on "procedural grounds" (e.g. incomplete or unsubstantiated claim), approx. 36% were resolved by "consumer education" (e.g. on how change information contact), approx. 15% feel into "other categories" (i.e. complaints relating to Privacy Shield companies, but not to their compliance with the Principles, such as billing/transactional issues).

[47] Under the Privacy Shield, the DoC has committed to provide an update to the DPA within 90 days after receipt of the complaint, to track (via the dedicated contact) all referrals from DPAs received by the DoC and to provide a report in the annual review analysing in aggregate the complaints received each year.

Individuals can also lodge complaints directly with the FTC under the same complaint system used by U.S. citizens.[48] As noted above, the FTC received three Privacy Shield-related complaints which however did not raise any issue of non-compliance with the framework. None of these therefore required follow-up actions by the FTC.

The FTC will also review complaints it receives from the DoC, DPAs and IRMs, by giving them priority consideration.[49] Similarly to the DoC, the FTC has set up a dedicated contact point (a "DPA Liaison") to liaise directly with the DPAs and a standard referral form to facilitate referrals and increase cooperation in the handling of individual complaints. No such referrals were reported during the first year of operation of the framework

4.1.3.4. The Binding Arbitration Mechanism

The Privacy Shield adds a new redress avenue for individuals: the Binding Arbitration Mechanism.[50] It is a mechanism of "last resort",[51] in case an individual considers that his/her complaint has not been satisfactorily resolved by any the other available redress mechanisms, to definitively establish whether a Privacy Shield company has violated its obligations under the Principles. Apart from lawyers' fees in case the individual decides to be represented by an attorney before the Privacy Shield Panel, this mechanism is free of charge for individuals with a fund being established to cover the arbitral costs. The decisions of the Privacy Shield Panel are binding and enforceable in U.S. courts. The Privacy Shield Panel has the authority to impose individual-specific, non-monetary relief (such as access, correction, deletion, or return of the individual's data in question) necessary to remedy the violation of the Principles. The arbitration procedure shall be completed within 90 days from the day on which notice has been delivered to the Privacy Shield-certified company concerned.[52]

Over the past year, a number of steps have been taken to make the arbitration mechanism operational.

First, the International Centre for Dispute Resolution of the American Arbitration Association (ICDR-AAA) was selected as the Arbitral Administrator and Fund Manager of the Binding Arbitration Mechanism. It will act as secretariat to the Panel.

Second, the Commission and the DoC have agreed on the Rules of Procedure and the Code of Conduct to govern the operation of the Privacy Shield Panel. These rules further specify important "consumer friendly" safeguards to the benefit of Europeans who would make use of this mechanism. This includes, in particular, the possibility of being assisted by a DPA in the preparation of the individual's arbitral notice (i.e. the individual's application), the provision to the individual of interpretation and translation at no cost, the clarification that individuals

[48] See www.ftc.gov/complaint
[49] See recital 54 and Annex IV to the adequacy decision.
[50] See recital 56 and Annex I (Annex 2) to the adequacy decision.
[51] Individuals may invoke arbitration only after having exhausted other avenues of redress such as bringing their complaint with the company, the independent recourse mechanism, or with the DoC. However, investigations by the FTC can proceed in parallel with arbitration.
[52] See recitals 56-58 and Annex I (Annex 2) to the adequacy decision.

may request discovery with respect to documents that are not otherwise available to him/her and that are "relevant and material to the outcome of the case", and transparent criteria for the designation of the arbitrators in case the parties cannot reach an agreement on the composition of the panel.

Third, to constitute the list of (at least) 20 arbitrators as requested by the framework, a first "Invitation for Applications for Inclusion on the List of Arbitrators" led to the selection of 16 arbitrators.[53] The arbitrators who were selected by the DoC and the Commission come from a variety of professional backgrounds, including legal practitioners with arbitration expertise, a former member of the judiciary, law professors from highly reputed academic institutions etc. They also represent different legal traditions, with arbitrators coming from the U.S., EU Member States as well as other third countries, and have demonstrated experience in U.S. privacy and EU data protection law. To select (at least) four additional arbitrators who would fully fulfil the framework's requirements, the DoC published a second "Invitation for Applications for Inclusion on the List of Arbitrators" in the U.S. Federal Register, with 6 October as deadline for submission. 16 applications were submitted and the final stage of the selection process is ongoing.

4.1.4. Enforcement by the Federal Trade Commission and the Department of Transportation

The Privacy Shield provides for stronger monitoring and enforcement obligations on the FTC (and the DoT) to make sure certified-companies live up to their commitments and that personal data continues to be protected after it is transferred to the United States.

On 8 September 2017, the FTC announced it had reached a settlement agreement with three companies charged for having falsely claimed participation in the Privacy Shield (the three companies had not yet completed the necessary steps for their certification while already claiming participation). These are the first cases brought by the FTC to enforce the Privacy Shield framework. The settlement prohibits misrepresentation about the companies' compliance with any privacy or data security program including the Privacy Shield.

The Commission services welcome these first actions taken by the FTC to enforce the Privacy Shield. However, it is expected that in the future the FTC will investigate not only false claims cases, but also Privacy Shield compliance issues on grounds of unfair or deceptive practices. In this respect, it would be important that the FTC develops a strategic and pro-active approach to enforcement, which would look "thematically" at how companies comply with certain obligations under the Privacy Shield, as it does in other areas of its enforcement activities by means of "sweep actions". In this respect, the Commission services note that during the review the FTC indicated that it was ready to make the Privacy Shield one of its priorities.

[53] The arbitrators serve a three-year term, which can be renewed once for an additional period of three years.

4.1.5. Substantive rules: the case of automated decision-making

Given the increasing use of automated processing (including profiling) as a basis for taking decisions affecting individuals in the modern digital economy, it has been agreed with the U.S. authorities that a dialogue on automated decision-making, including an exchange on the similarities and differences in the EU and U.S. approaches in this regard, is part of the first annual review as well as of subsequent reviews, if appropriate.[54]

Based on the limited feedback that the Commission has received, namely from trade associations during the preparation of the annual review and from business representatives at the relevant session of the Annual Joint Review itself, it appears that automated processing tends to be more relevant for processing by companies that are EU customer-facing, *i.e.* situations where personal data is collected directly from EU individuals by companies (including U.S. ones) operating in the European market. The entry into application of the GDPR in May 2018 will further clarify that these situations are generally covered by EU rules as, in particular, companies outside the EU that offer goods or services to European individuals (or monitor their behaviour) will be subject to the GDPR.[55] This includes the right for the individual not to be subject to a decision based solely on automated processing, including profiling, and which produces legal effects concerning him or her. When, by derogation to this prohibition, such type of processing is authorised by the GDPR, it should be subject to suitable safeguards which should include the right of the individual to obtain human intervention as well as the possibility to express his/her opinion and contest the decision.[56]

In the context of the annual review, the Commission services have also been informed in more detail about the safeguards that U.S. law would offer to EU individuals if automated decision-making takes place in the U.S. using personal data that has been transferred under the Privacy Shield. Such safeguards are provided in particular by the Fair Credit Reporting Act and by the Equal Credit Opportunity Act, which have also been taken into account in the Commission's adequacy decision.[57] The information received at the Annual Joint Review helped clarifying that the scope and application of the protections provided, in particular, by the Fair Credit Reporting Act, cover not only credit decisions but also other decisions affecting individuals, such as in the field of housing or employment, and which may be taken on the basis of automated processing.

The Commission services consider that further information is needed on the issue of automated decision-making and its relevance for the Privacy Shield. In view of continuing the dialogue, including at the next annual review - and before further steps may be considered - the Commission services will carry out an in-depth study which maps the situation and provides for reliable evidence, including on the similarities and differences in the EU and U.S. approach.

---

[54] Recital 25 of the adequacy decision.
[55] See Article 3(2) of the GDPR.
[56] See Article 22 and recital 71 of the GDPR.
[57] Recital 25 of the adequacy decision.

4.1.6. Relevant developments in the U.S. legal system

Under the Privacy Shield, the U.S. authorities have committed to inform the Commission about any legal development that could impact the functioning of the Privacy Shield, in the field of data protection, but also as regards the limitations and safeguards with respect to government access and use to personal data transferred under the framework.[58] Such developments can arise in a number of different areas, from changes in the legal framework (statutes, agency rules, etc.), to new jurisprudence by U.S. courts, to developments in agency practice when applying the law.

This commitment must be read in the light of the Commission's obligation to ensure the on-going monitoring of the situation in third countries for which it has made an adequacy finding,[59] which for the Privacy Shield has been specifically laid down in Article 4(1) of the adequacy decision.[60] Hence, the question of what constitutes a "material" development in the sense of the U.S. commitment should not depend on whether, ultimately, it negatively affects the functioning of the Privacy Shield, but rather on whether it is liable to raise questions about the protections afforded under the framework.

This past year was a year of change for the U.S., with a new administration and a new majority in Congress. Certain of the initiatives and measures taken in this new context raised some concerns from a privacy perspective. The NGOs consulted in preparation of the annual review stressed their apprehension that these might be the prelude to policy changes that could seriously impact the Privacy Shield.

The Commission has followed these developments with great attention over the course of the past year and will continue to monitor the situation. It considers that so far none of these developments affect the privacy protective framework created by the Privacy Shield. During the annual review, the U.S. authorities provided further explanations that supported this conclusion.

This concerns, in particular, the repeal by Congress in March 2017 of the privacy rules for internet service providers that the Federal Communications Commission (FCC) had proposed, a development which raised concerns among many stakeholders. It should be recalled from the outset that, as these FCC broadband privacy rules were not in force at the moment of the adoption of the Privacy Shield, they were not part of the Commission's adequacy assessment and thus their revocation could not have affected its findings. Moreover, as confirmed by the FTC during the annual review, if the proposed privacy rules had entered into application, they would not have been relevant for Privacy Shield-certified companies as only companies falling within the jurisdiction of the FTC (rather than the FCC) are eligible to participate in the Privacy Shield framework.

---

58 Recital 146 and Annex I (Annex 1) to the adequacy decision.

59 See *Schrems*, para. 76. This obligation has also been enshrined in Article 45(4) of the GDPR.

60 See recital 146 of the adequacy decision ("*To facilitate this process, the U.S. has committed to inform the Commission of material developments in U.S. law …*").

Another development discussed during the annual review is the *FTC vs AT&T* case which is currently pending before the U.S. Court of Appeals for the Ninth Circuit. The Court will decide whether to confirm or not an earlier decision which in August 2017 concluded that the FTC should be barred from regulating the non-common carrier activities of a company that qualifies as a common carrier (i.e. a telecom company) regulated by the FCC. In essence, the judgment to be issued in this case will delineate the frontier between the jurisdiction of the FTC and that of the FCC. It may therefore affect the coverage of the Privacy Shield (in that certain companies may no longer be able to adhere to the framework), but not the effectiveness of the personal data protections provided by the Privacy Shield.

The Commission services welcome these explanations. It is however expected that in the future the U.S. authorities provide the necessary clarifications in a more timely and proactive fashion, and not only in response to queries from the Commission.

4.2. ASPECTS RELATING TO ACCESS AND USE OF PERSONAL DATA TRANSFERRED UNDER THE PRIVACY SHIELD BY U.S. PUBLIC AUTHORITIES

The Principles set out in Annex II to the adequacy decision apply to companies that have received personal data transferred from the EU under the Privacy Shield, not to U.S. public authorities. At the same time, according to Annex II, Section 1.5, adherence to the Principles by Privacy Shield-certified companies may be limited to the extent necessary to meet national security, law enforcement or other public interest requirements.[61] Such companies thus have to allow U.S. public authorities the access to and use of personal data stored or otherwise processed by these companies in the United States following the transfer, if so required (and if this is necessary) for the above mentioned purposes.

With respect to an equivalent derogation in the Safe Harbour arrangement, the Court of Justice in its *Schrems* ruling criticised that the Commission's adequacy decision regarding that framework did not contain any findings as regards the limitations and safeguards applicable within the United States that would restrict the ability of U.S. public authorities to collect and use personal data.[62] The Court also specified the standards for public interest interferences in the EU legal order which constitute the benchmark against which to assess whether a third country provides an "*essentially equivalent*" level of protection,[63] bearing in mind that a third country may use different means to ensure such protection, as long as those means prove, in practice, to be effective[64]. In particular, the Court stressed that EU legislation involving such interferences needs to impose minimum safeguards, so that the persons whose personal data is concerned have "*sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data*."[65]

---

61 Annex II, Section 1.5 of the adequacy decision.
62 *Schrems*, paras. 82 to 89.
63 *Schrems*, paras. 91 *et seq*., in particular para. 96.
64 *Schrems*, para. 74.
65 *Schrems*, para. 91.

To reflect the requirements set out by the Court of Justice, the Commission's adequacy decision on the Privacy Shield contains a detailed assessment of the limitations and safeguards available in U.S. law as regards the collection and use by U.S. public authorities of personal data transferred under the Privacy Shield. Furthermore, the framework builds on written representations and assurances from the U.S. government (reflected in several annexes to the adequacy decision) to this regards.[66] The U.S. government has also committed to create a new mechanism for individual redress in the area of national security, the Privacy Shield Ombudsperson.

4.2.1. Limitations and safeguards regarding the collection and use of personal data for national security purposes

Based on its analysis and on the specific representations and commitments received from the U.S. Office of the Director of National Intelligence (ODNI) contained in Annex VI to the adequacy decision, the Commission has reached the conclusion that the U.S. rules limiting the collection and use of personal data, transferred from the EU to the U.S. under the Privacy Shield, for national security purposes provide an adequate level of protection. In particular, they do not allow the collection and subsequent use of electronic communications "*on a generalised basis*".[67]

The abovementioned finding of the Commission relies both on Presidential Policy Directive 28 (PPD-28) issued in 2014, which imposes a number of limitations and safeguards for signals intelligence operations in general, and specific statutory limitations and safeguards, in particular those stipulated in the Foreign Intelligence Surveillance Act (FISA). The ODNI has confirmed that PPD-28 applies to all U.S. signals intelligence activities, regardless of the legal authority on which such activities are based, and specifically contains protections for non-U.S. persons (including Europeans).[68]

4.2.1.1. Limitations and safeguards based on Presidential Policy Directive 28

According to PPD-28, signals intelligence may only be collected when there is a valid foreign intelligence or counterintelligence purpose and to the extent that the information cannot be obtained by other means, for instance from public sources. Furthermore, the collection of signals intelligence must always be as tailored as feasible, *i.e.* focused on specific foreign intelligence targets through the use of selectors (e.g. specific communication facilities such as an e-mail address). This means that targeted collection is the rule, whereas bulk collection (without the use of discriminants) may occur only in exceptional circumstances when targeted collection is not possible due to technical or operational reasons. Moreover, the Privacy Shield rests on specific representations and assurances from the ODNI according to which,

---

66 See also Annex I (Annex 1) to the adequacy decision, p. 44, according to which "*the information in these letters provides assurance to conclude that the Privacy Shield will operate appropriately, in accordance with the Principles therein.*" As shown by the header under which that statement is included, this links directly to the exceptions stipulated in Annex II, Section I.5 of the adequacy decision.

67 See *Schrems*, paras. 93, 94.

68 ODNI representations, Annex VI to the adequacy decision, p. 91.

even in the exceptional case of bulk collection, the U.S. intelligence agencies apply methods and tools to filter signals intelligence in order to focus it on the foreign intelligence sought and minimise the collection of non-pertinent information. Finally, the Commission has received assurances that, overall, bulk collection touches "*only a fraction of the communications traversing the Internet*".[69]

These principles are further specified in the policies and procedures that implement PPD-28 for individual intelligence agencies. As an example of such policies and procedures, the U.S. authorities referred the Commission to the National Security Agency (NSA)'s procedures issued under Section 4 of PPD-28.[70]

Section 4.1 and 4.2 of the NSA's Supplemental Procedures for the Collection, Processing, Retention and Dissemination of Signals Intelligence Information and Data containing Personal Information of Non-United States Persons confirm that "*SIGINT activities shall be as tailored as feasible*" and that "*whenever 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).*" Moreover, Section 4.2 clarifies that, "*if a collection method is regulated by FISA, the collection method will not be employed until the collection has been authorized in the manner prescribed by FISA.*" This includes both targeting and minimization procedures (see below, Section 4.2.1.3). Likewise, the policy and procedures for the Central Intelligence Agency (CIA) provide that, when engaging in signals intelligence collection, the CIA should, whenever practicable, conduct targeted intelligence collection rather than bulk collection. They further specify that collection activities should, whenever practicable, be directed against specific foreign intelligence targets or topics through the use of discriminants (e.g., specific facilities, identifiers, selection terms, etc.).

The ODNI's latest progress report on the implementation of PPD-28[71] states that the ODNI has completed and publicly released a standard for the whole Intelligence Community which establishes the process for reporting compliance issues involving personal information under PPD-28 to the Director of National Intelligence (DNI), and that other intelligence agencies, in particular the NSA, have undertaken significant efforts to train their personnel on PPD-28 requirements. The Commission services welcome these activities and note their importance in ensuring that the limitations and safeguards imposed by PPD-28 are complied with in practice.

Given its general scope of application and the fact that it has been specifically designed to provide protections to non-Americans, PPD-28 is a central element of the Commission's

---

69 ODNI representations, Annex VI to the adequacy decision, p. 207.

70 Section 4 of PPD-28 obliges all elements of the U.S. Intelligence Community to update or issue new policies and procedures as necessary to implement this Section. Other elements of the Intelligence Community have adopted equivalent agency policies and procedures.

71 ODNI Signals Intelligence Reform 2016 Progress Report, available on https://icontherecord.tumblr.com/ppd-28/2016.

finding that interference by U.S. authorities for national security purposes with personal data received from the EU by Privacy Shield-certified companies complies with the necessity test. It is thus of major importance that PPD-28 remains in place. During the annual review, the U.S. authorities, represented by the ODNI, expressly confirmed that both PPD-28 and all its implementing procedures are in place and that the current U.S. Administration "*is not making any change to PPD-28*."[72]

4.2.1.2. Electronic surveillance inside the United States requires Congressional authorisation through statute

In the adequacy decision, the Commission concluded[73] that, once personal data has been transferred to Privacy Shield-certified companies, U.S. intelligence authorities may only collect such data based on FISA or one of the statutes that authorise the use of so-called National Security Letters (NSLs).[74]

In their submissions sent to the Commission in preparation of the annual review, NGOs have raised concerns with respect to signals intelligence collection under Executive Order (E.O.) 12333. At the Annual Joint Review, the Commission therefore asked the U.S. authorities for further clarifications on this point, especially its relevance for the Privacy Shield. The U.S. authorities (ODNI/DoJ) confirmed that the collection of personal data for national security purposes from companies that have received such data under the Privacy Shield framework can only take place based on FISA[75] or one of the statutory bases for NSLs, in line with the Commission's findings.[76] They also stressed that does not allow circumventing these specific statutory authorisations for surveillance.[77]

This is an important confirmation because the USA FREEDOM Act prohibits bulk collection through the use of NSL or based on Sections 402, 501 FISA. The remaining legal authorizations for electronic surveillance under FISA are Section 104 for "traditional" surveillance based on an individualised warrant, and Section 702 through the use of specific selectors in line with court-approved targeting procedures (see below, Section 4.2.1.3).[78]

---

[72] Previously, House Representative J. Sensenbrenner, Chairman of the Subcommittee on Crime, Terrorism, Homeland Security and Investigations of the House Judiciary Committee, had stressed that PPD-28 "*is a foundation for the Privacy Shield*" and therefore urged the White House to retain it. See Letter of J. Sensenbrenner to (then) President-elect D. Trump of 20 December 2016.

[73] Recital 78 of the adequacy decision.

[74] These statutes are specifically listed in FISA, see 50 U.S.C. § 1873(e)(3). As indicated in footnote 80 of the adequacy decision, the most relevant legal authorization appears to be the Electronic Communications Privacy Act (18 U.S.C. § 2709).

[75] See also 965 F.Supp.2d 1090 (2013), *Jewel v. National Security Agency* ("*Through explicit provisions of FISA, Congress established a comprehensive, detailed program to regulate foreign intelligence surveillance in the domestic context*"; quoting 564 F. Supp.2d 1109, 1118 (N.D. Cal. 2008), *In re N.S.A. Telecommunications Records Litig.*).

[76] See also 50 U.S.C. § 1812 which clarifies that the existing statutory authorisations, in particular FISA, provide the "*exclusive means by which electronic surveillance and the interception of domestic wire, oral, or electronic communications may be conducted*."

[77] Moreover, any collection of data from the transatlantic cables during transmission to the U.S. would be subject to the requirements of PPD-28. See ODNI representations, Annex VI to the adequacy decision, p. 94.

[78] See recitals 78 to 81 of the adequacy decision.

4.2.1.3. Specifically: Surveillance under Section 702 FISA

Section 702 of FISA is of particular relevance for the personal data of Europeans that have been transferred from the EU to Privacy Shield-certified companies in the U.S., as it authorises the acquisition of foreign intelligence information through the targeting of non-U.S. persons located outside the U.S. with the compelled assistance of U.S. electronic communication service providers.[79]

While signals intelligence activities taking place on the basis of Section 702 FISA are also subject to the limitations and safeguards of PPD-28 (which "supplements" this statutory authorization), Section 702 itself contains a number of conditions and limitations aimed at ensuring targeted collection.

Firstly, targeting procedures ensure that the collection takes place only as authorised by FISA and remains within the scope of the certification. Collection is targeted through the use of individual selectors which identify specific communications facilities, such as an e-mail address or telephone number, and which U.S. intelligence personnel have determined are likely being used to communicate foreign intelligence information of the type covered by the certification.[80]

In this respect, the Commission services welcome the recent declassification of the procedures used by the NSA for targeting non-U.S. persons pursuant to Section 702 FISA.[81] Despite significant redactions, the non-redacted sections of these procedures show that the targeting procedures do not only aim at excluding U.S. persons from being targeted, but that NSA

---

[79] The term "electronic communication service provider" is defined in 50 U.S.C. § 1881 (a)(4). The acquisition of foreign intelligence information under Section 702 FISA takes place on the basis of annual certifications submitted to and approved by the Foreign Intelligence Surveillance Court (FISC). These certifications identify specific categories of foreign intelligence to be collected, such as intelligence related to international terrorism or weapons of mass destruction, which must fall within the categories of foreign intelligence defined by FISA. The certifications are also required to include targeting and minimization procedures which are to be approved by the FISC, see 50 U.S.C. § 1881a (c)(1)(A).

[80] This also applies in the case of so-called "upstream collection". As explained by the PCLOB, even though the methods applied differ, *"[t]he process of tasking selectors to acquire Internet transactions is similar to tasking selectors to PRISM*" in that "*selectors tasked for upstream Internet transaction collection must be specific selectors (such as an email address), and may not be key words or the names of targeted individuals."* According to the PCLOB, *"selectors used for the acquisition of upstream Internet transactions are sent to a United States electronic communication service provider*" and Internet transactions "*are first filtered to eliminate potential domestic transactions, and then are screened to capture only transactions containing a tasked selector. Unless transactions pass both these screens, they are not ingested into government databases.*" See PCLOB, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, 2 July 2014, pp. 36-37.

[81] Procedures used by the National Security Agency for targeting non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information pursuant to Section 702 of the Foreign Intelligence Act of 1978, as amended, of 30 March 2017 (NSA targeting procedures).

personnel[82] is also required to assess, based on the totality of the circumstances, that the target is expected to possess, receive, and/or is likely to communicate foreign intelligence information (and to provide a written explanation in this regard, to be checked by the DOJ and DNI). This assessment "*must be particularized and fact-based, informed by analytic judgment, the specialized training and experience of the analyst, as well as the nature of the foreign intelligence information expected to be obtained*."[83] Moreover, the procedures clarify that, "*[w]hen NSA proposes to direct surveillance at a target, it does so because NSA has already learned something about the target or the facility or facilities the target uses to communicate*."[84]

During the annual review the U.S. informed the EU side that, in order to ensure that these procedures are followed in practice, the NSA runs a compliance program and commits to report to the DoJ, the ODNI Office of the General Counsel and the ODNI Civil Liberties Protection Officer any incidents of non-compliance (including overcollection by any electronic communication service provider to whom a Section 702-collection request has been issued).[85] In addition, the NSA itself (like any other intelligence agency) is required to report compliance incidents to the FISC which on this basis can carry out its oversight function.[86]

Secondly, while mainly aimed at preventing the acquisition, retention and dissemination of information concerning U.S. persons, minimisation procedures also provide protections for non-U.S. persons by limiting the collection (acquisition) of data with respect to a specific foreign intelligence purpose, restricting access to databases in which information acquired under Section 702 FISA is stored (including through access controls) and by imposing limits on the use, retention and dissemination of such information.

The minimisation procedures used by the NSA in connection with the acquisition of foreign intelligence information pursuant to Section 702 FISA, dated 30 March 2017,[87] specify *inter alia* that the acquisition of such information will be conducted in a manner designed, to the greatest extent reasonably feasible, to minimise the acquisition of information not relevant to the authorised purpose of the acquisition.[88] Also, once acquired, search terms (e.g. key words) must be limited to those selectors that are "*reasonably likely to return foreign intelligence information*".[89]

---

82 According to information provided to the Commission at the Annual Joint Review, the NSA employs some 300 staff charged with the oversight over the intelligence authorities, including the review of tasking decisions.

83 NSA targeting procedures, pp. 4, 8.

84 NSA targeting procedures, p. 2.

85 NSA targeting procedures, pp. 8-9.

86 See recital 109 of the adequacy decision with reference to Rule 13(b) of the FISC Rules of Procedure. In addition, intelligence authorities are also overseen by the ODNI, DoJ and the competent Inspector-General (see 50 U.S.C. § 1881(a) (l)(2) and NSA targeting procedures, pp. 8-9).

87 Minimization procedures used by the National Security Agency in connection with acquisitions of foreign intelligence information pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended, of 30 March 2017 (NSA minimization procedures).

88 NSA minimization procedures, p. 3.

89 NSA minimization procedures, p. 4.

The application of the "targeting" and "minimization" safeguards contained in FISA is illustrated by a declassified FISC Opinion in which the Court analysed whether the protections afforded under the targeting and minimisation procedures had been respected. This demonstrates that the FISC does not merely review the targeting and minimisation procedures at the certification stage, but subsequently also examines how the procedures are being implemented.

FISC Memorandum, Opinion and Order of 26 April 2017 concerned a case of (inadvertent) non-compliance with the NSA's minimization procedures involving queries of data acquired under Section 702 FISA using U.S. person identifiers.[90] The fact that such non-compliance carried on for several years – albeit in the case at hand not with respect to the protections offered to non-U.S. persons – is a cause of concern. At the same time, it should be noted that according to the Order it was the U.S. government itself that had "*apprised the Court of significant non-compliance with the NSA's minimization procedures*" and "*made a written submission regarding those compliance problems*" in October 2016.[91] The Order also indicates that the non-compliance was discovered further to an NSA Inspector-General review and NSA Office of Compliance for Operations verification activities.[92] The Order cites the government as reporting that it was "*working to ascertain the cause(s) of those compliance problems and develop a remedial plan to address them*."[93] The Order thus provides evidence that oversight worked and compliance issues were addressed (albeit with some delay).

As a consequence of the abovementioned compliance incident, the NSA has stopped its so-called "about" collection under the "upstream" collection program[94] which is being operated under Section 702 FISA.[95] "About" collection refers to the collection not only ofcommunications *to* or *from* a Section 702 selector (such as an email address), but also of communications that contain a reference to such a selector (e.g. email communications which are not sent to or from the selected email address, but which include the selected email address in the text or body of the email) and are thus *about* the communication selectors of targeted persons.[96] During the Annual Joint Review, the ODNI reported that the elimination of "about" collection has led to a significant reduction of the number of communications collected under Section 702 FISA.

The FISA Amendments Act of 2008 which enacted Section 702 FISA is subject to a sunset clause and scheduled to expire at the end of 2017, unless re-authorised by Congress. The

---

90 FISC Memorandum, Opinion and Order of 26 April 2017 https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf.

91 FISC Memorandum, Opinion and Order of 26 April 2017, p. 4.

92 FISC Memorandum, Opinion and Order of 26 April 2017, p. 14-15.

93 FISC Memorandum, Opinion and Order of 26 April 2017, p. 4.

94 Upstream collection does not occur with the compelled assistance of U.S. electronic communication service providers, but of providers that control the internet backbone over which communications transit across the U.S. The collection thus does not rely on the local provider with whom the targeted person interacts, but on the flow of communications between communication service providers. PCLOB, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, July 2, 2014.

95 NSA statement of 28 April 2018, "NSA Stops Certain Section 702 "Upstream" Activities".

96 PCLOB, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, July 2, 2014.

upcoming debate on re-authorisation provides the U.S. Administration and Congress with a unique opportunity for strengthening the privacy protections in FISA. In this context, it is hoped that Congress will consider favourably enshrining important limitations and safeguards for signals intelligence applicable to non-U.S. persons on the basis of PPD-28 in FISA, which would ensure the stability and continuity of these protections. Any further reforms, both in terms of substantive limitations and procedural safeguards, should be implemented in the spirit of PPD-28 and therefore provide protection irrespective of nationality or country of residence.[97]

4.2.2. Surveillance activities in practice: figures and trends

During the preparations of the annual review, some of the NGOs that the Commission had asked to provide their views on the functioning of the Privacy Shield have voiced concerns about large-scale surveillance of communications data, and more specifically about a lack of targeting, allegedly leading to access to such data on a generalised basis. During the annual review, the Commission has therefore also sought to obtain quantitative elements of validation which could help to assess whether the limitations to the collection of signals intelligence contained in PPD-28 and FISA work in practice.

According to the ODNI's Statistical Transparency Report Regarding Use of National Security Authorities for Calendar Year 2016, issued in April 2017, there has been a slight decrease of the number of orders under Titles I and III of FISA (called "traditional FISA" as this concerns court orders to target individuals based on "probable cause") and of the number of targets from CY2015 to CY2016 (both remain well below 2,000). At the same time, the number of targets for orders under Section 702 FISA increased from 94,368 in CY2015 to 106,469 in CY2016.[98] During the annual review, the U.S. authorities explained that this increase could be explained by several factors, including changes in technology, communications patterns, target behaviour, national security threats and intelligence priorities.[99] As concerns National Security Letters – which may concern different types of records, not all of which are directly relevant for the Privacy Shield – the total number has further decreased from 12,870 in CY2015 to 12,150 in CY2016 (and significantly down from 19,212 in CY2013).[100] The

---

97 See PPD-28, Sec. 4, according to which "U.S. signals intelligence activities must, therefore, include appropriate safeguards for the personal information of all individuals, regardless of the nationality of the individual to whom the information pertains or where the individual resides".

98 This followed a moderate increase of the number of targets in previous years: from 89,138 in CY2013 to 92,707 in CY2014 to 94,368 in CY2015.

99 While the U.S. authorities did not provide further explanations, it appears plausible that for instance the number of communications facilities (e-mail accounts, social networks, etc.) used per individual is on average increasing (change in communication patterns). Likewise, the threat environment is evolving, with an increased risk for instance from ISIS activities – or, more generally, terrorist attacks – in recent years (changes in national security threats).

100 The number of "requests for information" is higher (24,801 in CY2016, down from 48,642 in CY2015), but the report explains that the FBI often issues NSLs under different legal authorities for the same individual or organisation, or might serve multiple NSLs for an individual for multiple facilities (e.g., multiple e-mail accounts): "*The number of requests, consequently, is significantly larger than the number of individuals or organisations that are the subjects of the NSLs*."

Commission services note that these numbers cover *all* foreign intelligence targets worldwide, not just Europeans.

Moreover, a number of U.S.[101] companies make use of the possibility provided for in the USA FREEDOM Act[102] to publish so-called transparency reports, which inform about the number of FISA and NSL access requests a company has received during a given reporting period. The companies that follow this practice include leading electronic communication service providers such as Google, Facebook, Yahoo!, Microsoft, Twitter and LinkedIn. During the reporting period January to June 2016, Microsoft, for example, received between 0 and 499[103] requests under FISA seeking the disclosure of communications content, which impacted between 12,000 and 12,499 user accounts.[104] In the same period, Facebook received between 500 and 999 requests for access to content under FISA, affecting between 13,000 and 13,499 user accounts,[105] while Google received between 500 and 999 such requests affecting between 25,000 and 25,499 accounts.[106] These figures illustrate that, as a percentage of total user accounts, the number of accounts affected by requests for government access to personal data remains limited.[107]

The publication of transparency reports is a helpful development. Companies are encouraged to make use of this opportunity to increase transparency and reassure their users.

To conclude, neither the figures and trends described above, nor the information on how the limitations and safeguards for the collection and use of personal data by U.S. public authorities provided in PPD-28 and FISA are applied in practice, indicate that the U.S. authorities do not comply with their representations and assurances. The Commission services will continue to monitor developments and will draw on all available sources of information, including the ODNI's annual report and companies' transparency reports, in future reviews.

4.2.3. Independent oversight

The U.S. intelligence community and its activities are subject to various review and control mechanisms. Aside from Congressional oversight, this includes in particular oversight within the executive branch and by the judiciary.

---

[101] According to information provided by Access Now, 68 companies had released transparency reports until autumn 2016, see: https://www.accessnow.org/transparency-reporting-index/.

[102] USA FREEDOM Act of 2015, Pub. L. No 114-23, Section 602(a), 603(a).

[103] Under the USA FREEDOM Act, numbers have to be presented in certain bands (e.g. 0-499, 500-999) to avoid that terrorists and other foreign intelligence targets can too easily find out which providers are most often the object of requests for surveillance, and thus avoid using their services.

[104] https://www.microsoft.com/en-us/about/corporate-responsibility/fisa/.

[105] https://govtrequests.facebook.com/country/United%20States/2016-H1/.

[106] https://transparencyreport.google.com/user-data/us-national-security.

[107] By way of comparison, for instance, Facebook in June 2017 reported having reached 2 billion users worldwide. See: http https://www.facebook.com/zuck/posts/10103831654565331 and https://www.reuters.com/article/us-facebook-users/facebook-hits-2-billion-user-mark-doubling-in-size-since-2012-idUSKBN19I2GG.

4.2.3.1. Inspectors General

In the adequacy decision, the Commission analysed in detail the relevant oversight mechanisms within the executive branch of the U.S. government.[108] At the annual review, the Commission obtained further information from the U.S. authorities on the oversight system, in particular the obligations of U.S. intelligence authorities to report compliance incidents[109] as well as the efforts undertaken to address such incidents (this includes re-training, but also disciplinary actions such as the dismissal of employees where necessary and appropriate).[110]

With respect to independent oversight, the Inspectors General (IGs) are of particular importance. As the Commission explained in the adequacy decision,[111] each Intelligence Community element has its own IG with responsibility, among others, to oversee foreign intelligence activities. IGs are statutorily independent and responsible for conducting general audits and individual investigations relating to the programs and operations carried out by the respective agency for intelligence purposes, including for abuse or violation of the law. They are authorised to have access to all records, reports, audits, reviews, documents, papers, recommendations and other relevant material, if need be by subpoena, and may take testimony. While the IGs can only issue non-binding recommendations for corrective action, their reports, including on follow-up action (or the lack thereof) are made public and moreover sent to Congress which can on this basis exercise its oversight function.

During the annual review, the Commission, as well as the representatives of the WP29, asked questions the General Counsel of the Inspector General of the Intelligence Community (IG GC) questions about the oversight role of the IG. This Inspector General has comprehensive jurisdiction over the entire Intelligence Community and is authorised to investigate complaints or information concerning allegations of unlawful conduct, or abuse of authority, in connection with ODNI and/or Intelligence Community programs and activities. In her presentation and in response to questions from the Commission and the WP29 representatives, the IG GC stressed both the independence of all IGs and their in principle "unfettered" access to information when carrying out an investigation.[112] While dismissal of an IG by the President is possible and the Attorney-General may deny access to "Federal grand jury materials" upon a determination that this would likely impede important public interests (e.g. interfere with an ongoing criminal investigation or pose a serious threat to national security),

---

[108] Recitals 93 to 101 of the adequacy decision.

[109] See already above Section 4.2.4. For the obligation to report compliance incidents to the DNI, see IC Standard 107-02 – Reporting Significant Compliance Issues Involving Personal Information under PPD-28 to the DNI; for the obligation to report compliance incidents to the Intelligence Oversight Board, see Section 1.6(c) of E.O. 12333; for the obligation to report compliance incidents to the FISC, see Rule 13(b) of the FISC Rules of Procedure.

[110] As regards the latter, the U.S. authorities submitted a letter of 11 September 2013 from the NSA to Senator Grassley of the U.S. Senate Committee on the Judiciary which lists 12 instances of intentional misuse of SIGINT authorities by NSA personnel in the 10 year-period since 1 January 2003, as well as the oversight actions taken in this respect.

[111] Recital 97 of the adequacy decision.

[112] As recently strengthened through the Inspector General Empowerment Act of 2016, Pub. L. 114-317, 16 December 2016, Section 5. According to the information received, IG staff has "appropriate clearance" to see classified information.

in both cases Congress must be informed, thereby ensuring parliamentary control against abuses. The IG GC stressed that no IG has ever been dismissed other than "for cause" (*i.e.*, misconduct) since this parliamentary control process was put in place and that they have their own, independent budget (under the control of Congress).

As regards oversight with respect to non-compliance, in reply to a question whether IGs also control the application of PPD-28 and/or the implementing agency rules, the IG GC confirmed that it checks compliance against all legal provisions (statutes, agency rules, etc.) that apply to the respective intelligence activities, irrespective of whether such provisions grant individual rights. This is a relevant clarification, in particular given the important role played by IGs as part of the Ombudsperson mechanism. According to the Inspector General Empowerment Act of 2016, whenever an IG issues a recommendation for corrective action to an agency, the document containing the recommendation will at the same time be submitted to the competent congressional committees. Moreover, unless disclosure is specifically prohibited by law, the same document shall immediately be made public on the IG's website.[113] This complements the IG's general obligation to semi-annually submit a report on their activities to Congress. The cooperation between the Ombudsperson and the IGs is described in Section 4.2.4.2 below.

4.2.3.2. The Privacy and Civil Liberties Oversight Board

The Privacy and Civil Liberties Oversight Board (PCLOB) is an independent agency within the executive branch which, according to its founding statute, consists of a bipartisan, five-member Board and supporting staff. It is entrusted with responsibilities in the field of counterterrorism policies and their implementation, with a view to protecting privacy and civil liberties. In its review of surveillance by U.S. intelligence agencies, the PCLOB may access all relevant agency records, including classified information, conduct interviews and hear testimony. It may issue recommendations to intelligence authorities, and regularly reports to Congressional committees and the President. According to Section 5(b) of PPD-28, the PCLOB is "encouraged", within the confines of its mandate, to prepare a report assessing the implementation of PPD-28.

The PCLOB's enabling statute provides that Board members are "*appointed by the President, by and with the advice and consent of the Senate*."[114] Three Board members constitute a quorum.[115] Currently, four of the PCLOB's five seats are vacant with only one Board member (E. Collins) remaining. The PCLOB's former Chairman resigned with effect of 1 July 2016, and three more members departed in early 2017 (one retired, and two had to leave due to term expirations). On 5 September 2017, President Trump nominated a new PCLOB Chairman, A.

[113] Inspector General Empowerment Act of 2016, Pub. L. 114-317, 16 December 2016, Section 4(d).
[114] 42 U.S.C. § 2000ee, Section (h)(1).
[115] 42 U.S.C. § 2000ee, Section (h)(5).

Klein,[116] who however still needs Senate confirmation before being able to take office. By the time of the Annual Joint Review, no further nominations had been reported.[117]

Following a letter by the Commission of 2 March 2017 enquiring about the status of the PCLOB, the U.S. authorities (DoJ) had reassured the Commission that the PCLOB can still carry out its functions through the remaining Board member together with the agency's permanent staff. This was confirmed during the Annual Joint Review by the remaining Board member of the PCLOB. While she acknowledged that the PCLOB currently cannot initiate new oversight projects and/or adopt reports in on-going investigations, she also stressed that the sub-quorum situation arose due to unforeseen circumstances (namely, the resignation of two Board members prior to the end of their term) and does not prevent the PCLOB from continuing its work on projects that were agreed at Board level before it lost its quorum. Moreover, the PCLOB can still issue advice/recommendations and individual Board members can testify before Congress, and this has indeed happened following the loss of quorum. Nevertheless, the Commission services remain concerned about the current Board situation which has as a consequence that the PCLOB is at least not fully functional.

As regards oversight projects that the PCLOB is known to be engaged in, the Board member explained to the Commission that the investigation into the use of E.O. 12333 is still on-going (with staff working on three "deep dives" into specific areas of application). Conversely, the report on the implementation of PPD-28 has been adopted and sent to the President. Although it was confirmed at the Annual Joint Review that the report has been checked from a national security point of view and certain parts are de-classified, it was also explained that this report cannot be released to the public, as it is currently subject to Presidential privilege. Given the relevance of PPD-28 for the limitations and safeguards applying to government access for signals intelligence, and thus for the Commission's regular review of its adequacy assessment, the release of the report by the U.S. authorities would be of particular importance.

4.2.4. Individual redress

The adequacy decision assesses in detail the redress avenues available to individuals when it comes to government interference for national security reasons.[118] These consist of several types of judicial remedies[119] as well as the Ombudsperson mechanism[120] that complements judicial redress.

[116] Available at: https://www.whitehouse.gov/the-press-office/2017/08/25/president-donald-j-trump-announces-intent-nominate-personnel-key.

[117] It should be noted that, since the PCLOB by law has a bi-partisan membership, the appointment of board members necessarily requires consultation with the opposition party (currently the Democrats in Congress).

[118] Separately, the decision also discusses individual redress for law enforcement purposes, see recitals 130 to 134 of the adequacy decision.

[119] Recitals 111 to 114 of the adequacy decision.

[120] Recitals 116 to 122 of the adequacy decision.

4.2.4.1. Judicial remedies available to EU individuals

In the adequacy decision, the Commission noted that U.S. law offers several avenues for judicial redress in the area of government surveillance open to all individuals irrespective of their nationality. Aside from actions under FISA[121] (50 U.S.C. §§ 1806, 1810) and the Electronic Communications Privacy Act (ECPA, 18 U.S.C. 2701-2712),[122] these include causes of action for specific types of data, targets and forms of access, such as under the Computer Fraud and Abuse Act (18 U.S.C. § 1030)[123] or the Right to Financial Privacy Act (12 U.S.C. § 3417).[124] In addition, two general types of action exist, namely under the Administrative Procedure Act (APA)[125] (for any person suffering "legal wrong", or adversely affected/aggrieved by agency action), and the Freedom of Information Act (FOIA)[126] (for access to documents).

During the preparatory phase of the annual review, some NGOs expressed concern about limited possibilities for judicial redress as well as difficulties to overcome the "standing" requirement stemming from Article III of the U.S. Constitution. The Commission therefore asked the U.S. authorities for additional information on the availability of judicial redress under APA (5 U.S.C. § 702) and FOIA (5 U.S.C. § 552), as well as the interpretation of the "standing" requirement by U.S. courts. In response, the U.S. authorities provided the Commission with a number of court decisions applying these legal bases as well as further explanations at the Annual Joint Review.

The materials provided to the Commission show that applicants, including foreigners,[127] have indeed been able to bring court actions against government surveillance based on the APA. For instance, in a case of 2015, *ACLU v. Clapper*,[128] the applicant alleged that the U.S. government's (in the meantime abolished) bulk collection of telephone metadata under Section 215 of the Patriot Act (*i.e.*, the business records provision of FISA, 50 U.S.C. § 1861) was unlawful. The U.S. Court of Appeals for the Second Circuit held that the APA did provide a means for the ACLU to seek redress for what it claimed was a government data access program that violated the requirements of FISA (and in particular that the APA action was not barred by other judicial remedies available under FISA). The Court went on to hold that the telephone metadata collection programme in fact violated the FISA statute.[129]

With respect to requests under FOIA, the U.S. authorities explained at the Annual Joint Review that this is an instrument often used by individuals (and increasingly so, given the

[121] Recital 112 of the adequacy decision.
[122] See recitals 112-113, 132 of the adequacy decision.
[123] See recitals 113, 134 of the adequacy decision.
[124] See recitals 113, 134 of the adequacy decision.
[125] See recitals 113, 131 of the adequacy decision.
[126] See recitals 114, 133 of the adequacy decision.
[127] See e.g. 814 F.Supp.2d 1087 (D.C. Cir. 2010), *Abdur-Rahman v. Napolitano*. While this case did not concern government access to data, it shows that also foreign applicants are entitled to seek redress under the APA.
[128] 785 F.3d 787 (2nd Cir. 2015), *American Civil Liberties Union v. Clapper*.
[129] The ACLU sought injunctive relief, but the court declined to immediately order the government to end the programme which was set to expire in any event. Shortly thereafter Congress adopted the USA Freedom Act which led to the (early) termination of the telephone metadata programme which ACLU had challenged.

transparency efforts by the U.S. government in the area of national security which provide "hooks" for applicants to seek access to further documents mentioned in the published material). In reply to questions from the Commission regarding the applicable exemptions, including based on national security considerations, the U.S. authorities acknowledged these limitations but pointed out that the use of the exemptions may be (and often is) challenged in court and that litigation often results in negotiated settlements leading to at least partial disclosure.[130] In this respect, it should also be noted that, according to U.S. jurisprudence, FOIA exemptions must be interpreted narrowly, consistent with the Act's goal of broad disclosure, and the public authority asserting the exemption bears the burden of proof for demonstrating that its conditions are fulfilled.[131]

Finally, the U.S. authorities have pointed to the notification requirement in FISA when the government intends to use FISA information in criminal and other legal proceedings brought against the individual.[132] While this safeguard only applies where information obtained through surveillance is used in such proceedings, it constitutes a further avenue of judicial redress enabling the court hearing the case to consider the question of the lawfulness of the surveillance measure, with implications beyond the individual case.

As regards the standing question, the adequacy decision already made reference to this limitation for judicial redress.[133] This being said, it must be recognised that all legal systems – including that of the EU and its Member States – contain procedural rules that restrict access to the courts on admissibility grounds and these limitations will be more difficult to overcome in the area of national security. Access to courts against government action typically presupposes a concrete indication that the rights of the individual have been violated, which in turn requires that the individual is aware of surveillance activities directed against him or her. As surveillance for national security purposes is conducted for threat prevention, often in the long term, rather than to investigate and punish past offences, notification of the individual is understandably subject to stricter conditions than in the area of law enforcement.

U.S. jurisprudence on the issue of standing in the case of government surveillance is still evolving. In this respect, the U.S. authorities have pointed the Commission to the proceedings in *Jewel v. National Security Agency*[134] and *Wikimedia v. National Security Agency*.[135] While

---

130 In fact, "*any segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt* […]." See 756 F.3d 100, 117 (2nd Cir. 2014), *New York Times Co. v. U.S. Dept. of Justice*. There is thus a requirement for partial disclosure, to the extent possible.

131 See 756 F.3d 100, 111-112 (2nd Cir. 2014), *New York Times Co. v. U.S. Dept. of Justice* ("*all doubts as to the applicability of the exemption must be resolved in favour of disclosure*").

132 18 U.S.C. §§ 1806(c), 1825(d), 1845 (c).

133 Recital 115 of the adequacy decision.

134 673 F.3d 902 (2011), *Jewel v. National Security Agency*.

135 857 F.3d 193 (4th Cir. 2017), *Wikimedia Foundation v. National Security Agency*. This case, which concerned a challenge to the lawfulness of FISA Section 702 Upstream collection, is based on publicly available information about how FISA Section 702 operates (including the PCLOB report) and Wikimedia's assertion that, given its large volume of global internet communications, it is extremely likely that some of its data has been intercepted through the Upstream program. The trial court granted the U.S. government's motion to dismiss for lack of standing, but the appellate court reversed that decision, finding that Wikimedia's allegations met the legal requirements of standing doctrine. The case will now proceed to a second stage to

these cases are not yet finally decided, they nevertheless suggest that, depending on the circumstances,[136] applicants can succeed at the admissibility stage.[137] In addition, the U.S. authorities have pointed to the requirement for notification that exists with respect to certain surveillance laws (e.g. the Wiretap Act) and which facilitates a showing of standing.

4.2.4.2. Individual redress through the Privacy Shield Ombudsperson mechanism

Moreover, as a means to facilitate access by individuals to independent review, the U.S. government has created the Privacy Shield Ombudsperson mechanism which specifically provides that "*the request needs not demonstrate that the requester's data has in fact been accessed by the United States Government through signal intelligence activities*" in order to be considered complete (thereby triggering an obligation for the Ombudsperson to provide a response to the individual "*in a timely manner*").[138]

The mechanism, which ensures that non-U.S. individuals can bring complaints with respect to U.S. intelligence measures and have them addressed by the Ombudsperson, is unique at international level. It includes the Privacy Shield Ombudsperson as well as other oversight bodies competent to oversee the different elements of the Intelligence Community, in particular the Inspectors General, on whose cooperation the Privacy Shield Ombudsperson will rely in dealing with complaints. As set out in Annex III to the adequacy decision, the Ombudsperson is independent from the intelligence services and the State Department – where the Ombudsperson is located – has committed to "*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*."[139] To this end, the U.S. State Department has included safeguards against improper influence in the procedural rules that govern the implementation of these commitments.[140] According to these rules, the Ombudsperson will report any attempts of improper influence – from inside or outside the State Department – directly to the Secretary of State, who will take the actions appropriate to ensure that the Ombudsperson can carry out its function objectively and free from improper influence. The Ombudsperson can also refer any such attempts to the appropriate IG.

The position of the Under-Secretary in the State Department to whom the office of the Ombudsperson has been assigned is currently vacant and it is not yet clear when the post will be permanently filled. President Trump has not yet announced the nomination of a candidate, who would still have to be confirmed by the Senate. Until the post is filled, J. Garber, one of the acting Assistant Secretaries, is Acting Ombudsperson. She relies on permanent staff that

---

further determine the trial court's jurisdiction over the case based on an analysis of the underlying evidentiary record.

136 See also for instance the case of *ACLU v. Clapper* (above footnote 129) in which the applicant could rely on leaked documents to demonstrate standing.

137 For a further case where a U.S. court dismissed a "facial" challenge to standing with respect to surveillance under the PRISM program, see 839 F.3d 336 (3d Cir. 2016), *Schuchardt v. President of the United States.*

138 Annex III, Sec. 3(c), 4(e) of the adequacy decision.

139 See recitals 116 to 122 of the adequacy decision.

140 Privacy Shield Ombudsperson Mechanism Unclassified Implementation Procedure.

supports the Ombudsperson office. The Commission services understand that the current vacancy is related to the transition from one U.S. Administration to the next, and that there are (many) other positions – in the State Department and elsewhere in the U.S. government – where appointments still have to be made. However, given the importance of the Ombudsperson mechanism for the Privacy Shield framework, and as a sign of the U.S. political commitment to the mechanism, the Ombudsperson should be appointed as soon as possible.

In terms of procedure, the WP29 and the Ombudsperson office have, since the adoption of the adequacy decision, worked closely together to establish a number of tools to facilitate the complaint process, from its filing to its referral to the Ombudsperson to the return of a reply. On the EU side, the Data Protection Authorities have designated the WP29 as the "EU Centralised Body" that will channel complaints – which can be filed with any DPA or other national body with oversight functions in the national security area – to the Ombudsperson. In this context, the WP29 has also drawn up the "Rules of Procedure for the Submission of Requests to Ombudsperson via the "EU Centralised Body" according to the EU-U.S. Privacy Shield" as well as a form for the submission of requests.[141] In turn, the U.S. State Department has established an online platform for the Ombudsperson[142] and prepared an electronic form through which the EU Centralised Body can transmit requests to the Ombudsperson. In addition, it has published a Federal Register Notice on a new system of records (the "Ombudsperson Mechanism Records") that shall assist the Ombudsperson in the overall management of the request review process and the provision of its response "*by facilitating accurate and up-to-date record keeping*".[143]

The procedural rules which govern the implementation the US commitments with regard to the Ombudsperson mechanism assign, among others, responsibilities within the Department and set out the steps in the review process, in particular as regards the determination as to whether a complaint is deemed sufficient to trigger a review under the Ombudsperson mechanism. This is the case if the complaint contains all the information needed for the it to be assessed, in particular a unique identifier associated with the type of communication that is the subject of the complaint, such as an email address or a telephone number. While the procedure that is followed if a complaint is deemed sufficient and further processed by the Ombudsperson remains classified, the procedural rules illustrate how the Ombudsperson will cooperate with the Intelligence Community and with independent oversight bodies to review such complaints. The Ombudsperson will forward the complaint to the Civil Liberties and Privacy Office of the intelligence agency to which the complaint pertains, as well as to the Office of the IG of the Intelligence Community (who can, on the basis of the complaint, conduct an independent review). The complaint will be reviewed first by the Civil Liberties and Privacy Office of the relevant intelligence agency and then forwarded to compliance officials for further review. Their findings are reported back to the Ombudsperson.

[141] Both are available on the WP29 webpage at: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.
[142] See at: https://www.state.gov/e/privacyshield/ombud/
[143] Federal Register, Vol. 82, No. 179 (18 September 2017).

If the review of a complaint reveals a violation of U.S. law (including executive orders and presidential directives), the Ombudsperson will make use of the existing oversight structure to ensure that the violation is remedied. Depending on the specific incident, such remedy may include the purging of data that has been unlawfully acquired. In addition, any case of non-compliance will be reported to the competent oversight bodies, which include the ODNI, the President's Intelligence Oversight Board, the PCLOB, the specific IG for the Intelligence agency in question, the intelligence oversight committees in Congress and the FISC.

At the Annual Joint Review, the current (Acting) Ombudsperson confirmed that for her to provide a reply (as set out in Annex III, Sec. 4(e) of the adequacy decision), she first has to be satisfied that no violation of U.S. law occurred or that the violation has been remedied. This confirms that she will always (have to) make her own assessment of the situation. At the same time, the IG GC informed the Commission that standardised procedures for case referral within the Executive Branch exist, that would also cover referrals from the Ombudsperson to the competent IG (which will then act as the office of inquiry). Following such a referral and the investigation of the request, the competent IG would then report back to the Ombudsperson.

4.2.5. Relevant developments in the U.S. legal system

Since the adoption of the adequacy decision on 12 July 2016 and the start of operation of the framework on 1 August 2016, the Commission became aware of a number of legal developments in the United States in the area of national security that could raise concerns from a privacy perspective. In each case, the Commission investigated the matter and concluded that its findings in the adequacy decision remain unaffected. This includes in particular the following developments:

- The new "Procedures for the Availability or Dissemination of Raw Signals Intelligence Information by the National Security Agency", issued on 3 January 2017 under E.O. 12333, expand the possibilities for the NSA to share raw signal intelligence information with other parts of the Intelligence Community. However, aside from the fact that these procedures do not apply to intelligence collected under FISA, a number of limitations and safeguards apply. For instance, the ODNI has explained that dissemination requires a reasoned request justifying the intelligence need and that the receiving U.S. intelligence authority must follow rigorous privacy policies (including strict oversight and compliance review). In particular, any information shared pursuant to these procedures is subject to the protections of PPD-28 and corresponding agency rules. On that basis, these increased possibilities to share data within the Intelligence Community do not appear to affect the findings made in the Commission's adequacy decision as regards the further dissemination of personal data of EU individuals transferred under the Privacy Shield and collected by means of signals intelligence.

- Rule 41 of the Federal Rules of Criminal Procedure has been expanded to allow for the issuing of warrants for remote access searches of devices the location of which is

unknown. As the Commission understands, this changes the rules for determining jurisdiction, by giving district court judges the authority to issue law enforcement warrants for searches that might take place outside their district court's jurisdiction. Conversely, it does not affect (expand) the power to conduct searches, or the warrant requirement, as such. While there have been suspicions that the new rules might also allow searches outside the U.S. (which has been refuted by the DoJ), this would in any event not be relevant for the Privacy Shield.

– Section 14 of E.O. 13768 "Enhancing Public Safety in the Interior of the United States" (issued by President Trump on 25 January 2017 as part of his reversal of immigration policies) provides that "*[a]gencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information*". In the Commission's view, this does not affect the Privacy Shield given that the adequacy assessment does not rely on the protections of the Privacy Act. Following a written request from the Commission, the DoJ has explicitly confirmed this analysis in writing by letter dated 22 February 2017.

These developments, which were also material in the sense explained, should have been reported by the U.S. authorities to the Commission, in line with their commitment under the framework. Only upon enquiries from the Commission did the U.S. government provide clarifications and reassurances.

Hence, the Commission services expect that in the future the U.S. authorities provide timely and comprehensive information about any development that could be of relevance for the Privacy Shield.

As regards possible future developments, two are particularly noteworthy:

– Due to a "sunset clause", Section 702 FISA will have to be reviewed by the end of 2017. This has raised concerns (especially among privacy NGOs) that the powers of the U.S. Intelligence Community to carry out surveillance might be expanded, and/or existing privacy protections be curtailed. In particular, concerns have been voiced that the NSA may request an amendment of Section 702 FISA to allow so-called "about" collection as part of its "Upstream" program.[144] On 7 September 2017, Attorney General Jeff Sessions and Director of National Intelligence Dan Coats asked the U.S. Congress for an unchanged and permanent re-authorisation of Section 702 FISA. On 4 October, the House Judiciary Committee circulated draft legislation to re-authorise and reform Section 702 FISA. The upcoming review of Section 702 FISA is an opportunity for the US Administration and Congress to consider enshrining important limitations and safeguards for signals intelligence applicable to non-U.S. persons on

[144] As indicated above (Section 4.1.2.3), the NSA had to stop "about" collection following an order by the FISC.

the basis of PPD-28 in the Foreign Intelligence Surveillance Act, as this would ensure the stability and continuity of these protections. Any further reforms, both in terms of substantive limitations and procedural safeguards, should be implemented in the spirit of PPD-28 and thus provide protection irrespective of nationality or country of residence.

– Finally, NGOs have expressed concerns that Congress may be considering ways to narrow the jurisdiction of the PCLOB to only cover the privacy and civil liberties of U.S. persons, and/or to limit the PCLOB's oversight functions. While the PCLOB is only one of the several existing oversight bodies that has been analysed in the adequacy decision, such changes – if realised – would weaken an important and independent actor of the overall check-and-balance system whose work has led to key reforms.

As each of these possible developments could be relevant to the Privacy Shield, the situation will continue to be closely monitored and the impact of any of these changes on the framework will be carefully assessed.