ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN

WP 255

EU – U.S. Privacy Shield – First annual Joint Review

Adopted on 28 November 2017

Executive summary

Introduction

According to the EU–U.S. Privacy Shield adequacy decision ("Privacy Shield")[1] adopted on 12 July 2016, **eight representatives of the WP29 participated in the first joint review conducted by the European Commission, on September 18 and 19, 2017** in Washington DC to assess the robustness of its adequacy decision.

Based on the concerns elaborated in its previous opinions, in particular opinion 1/2016, the WP29 focused on the assessment of both the **commercial aspects** of the Privacy Shield and on the **government access to personal data transferred from the EU for the purposes of Law Enforcement and National Security, including the legal remedies available to EU citizens**. The WP29, assessed whether these concerns have been solved and also whether the safeguards provided under the EU-U.S. Privacy Shield are workable and effective.

The WP29's main findings of this joint annual review, stemming both from written submissions, and from oral contributions, are hereby presented in this report aside from the European Commission's report[2].

On the commercial aspects of the Privacy Shield

The WP29 welcomes the various efforts made by US authorities **to set up a comprehensive procedural framework to support the operation of the Privacy Shield** through for example the **strengthening of the checks performed** prior to the listing of certified organizations.

However, the WP29 has identified **a number of important unresolved issues** such as the **lack of guidance and clear information** on, for example, the principles of the Privacy Shield, on onward transfers and on the rights and available recourse and remedies for data subjects. In addition, the WP29 calls for **an increased oversight and supervision of compliance with the Principles of the Privacy Shield** through namely, ex-officio investigations and continuous monitoring of certified companies. The US authorities are also requested to clearly **distinguish the status of data processors from that of data controllers** both at the time of their self-certification and at the time of further checks.

Moreover, further improvements should be made with regards **to the interpretation and handling of HR data and the rules governing automated-decision making/profiling**. Finally, the **self-certification process for companies** should be enhanced to ensure uninterrupted protection for data subjects and rapid compliance with the Privacy Shield principles. Additionally, **the cooperation between U.S. authorities within the Privacy Shield mechanism** should be adjusted.

In addition to the points mentioned above, the WP29 recalls the unresolved issues mentioned in Opinion 1/2016, e.g. **absence or limitation** to the rights of the data subjects, of key definitions, of guarantees on transfers for regulatory purpose in the field of medical context and the overly broad exemption for publicly available information.

[1] 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.

[2] 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; 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, Brussels, 18.10.2017 SWD(2017) 344 final

On the access by public authorities to data transferred to the U.S. under the Privacy Shield

The WP29 **welcomes the efforts made by the U.S. government and legislator to become more transparent on the use of their surveillance powers** by publishing a number of important documents, for example, decisions by the Foreign Intelligence Surveillance Court (FISA Court), in part by declassification.

Despite these developments, **some of the main points of concern for the WP29 in this area, have yet to be fully resolved**.

More specifically, the c**ollection and access of personal data for national security purposes** under both section 702 of FISA and Executive Order 12333 still remains an important issue for the WP29.

Indeed, the WP29 calls for **further evidence or legally binding commitments** to substantiate the assertions by the U.S. authorities that the collection of data under section 702 is not indiscriminate and access is not conducted on a generalized basis under the UPSTREAM program.

Furthermore, the **Privacy and Civil Liberties Oversight Board (PCLOB)** should be in a position to prepare and issue an updated report building on the report issued in 2014 further assessing the necessity and proportionality of the definition of "targets" and of the tasking of selectors under **section 702** (including in the context of the **UPSTREAM program** should it be maintained), as well as the concrete process of application of selectors in the context of the UPSTREAM program to clarify whether massive access to data occurs in this context. In addition, the WP 29 regrets that the report on **Presidential Policy Directive 28 (PPD28)** is still subject to Presidential privilege and is thus not published yet.

With the imminent decision on whether and how to **re-authorize section 702 FISA** by the end of this year, the WP 29 takes the view that if Section 702 were to be reauthorized, several improvements should be introduced. Instead of authorizing surveillance programs, section 702 should provide for precise targeting, along with the use of the criteria such as that of "reasonable suspicion", to determine whether an individual or a group should be a target of surveillance, subject to stricter scrutiny of individual targets by an independent authority ex-ante.

Concerning the application of **Executive Order 12 333** to EU data transferred to the U.S., the PCLOB should be in a position to finish and issue its awaited report on EO 12 333 to provide information on the concrete operation of this Executive Order and on its necessity and proportionality with regard to interferences brought to data protection in this context.

With respect to oversight, the **rapid appointment** of new members to the vacancies on the Privacy and Civil Liberties Oversight Board (PCLOB) is essential to ensure effective control and monitoring.

The redress by EU citizens before U.S. courts is still to be effectively guaranteed due to the problematic admissibility threshold of the **"standing requirement**". Therefore, the WP29 will continue to follow closely the evolution of the case law.

Hence, the Ombudsperson is a key element that is designed to compensate the above-mentioned lack or uncertainty to seek effective redress before court. In any way the Ombudsperson **shall be appointed as soon as possible**.

Also, the exact powers of the Ombudsperson mechanism need to be clarified through the **declassification of internal procedures** concerning the interactions between the Ombudsperson and the other elements of the IC or oversight bodies. Based on the information provided, the WP29 is of the view that the powers of the Ombudsperson to remedy non-compliance vis-à-vis the intelligence authorities are not sufficient in the light of Article 47 EU Charter of Fundamental Rights. The Ombudsperson should also be able to bring the matter before Court.

Finally, regarding the **access to data for law enforcement purposes** the WP29, underlines its remaining concerns on the available effective remedies for individuals in cases where the data of companies will have been accessed by law enforcement authorities.

Conclusion

The WP29 acknowledges the **progress of the Privacy Shield in comparison with the invalidated Safe Harbor Decision**. The WP29 recognizes the efforts made by the U.S. authorities and the Commission to implement the Privacy Shield. To complement these efforts, the WP29 will engage in advising the U.S. authorities in drafting new guidance, in particular regarding HR data and onward transfers, in order to develop a common understanding of the Privacy Shield Principles and to address the needs of the business community on both sides of the Atlantic.

However, **the WP29 has identified a number of significant concerns that need to be addressed by both the Commission and the U.S. authorities**. **Therefore the WP29 calls upon the Commission and the U.S. competent authorities to restart discussions**. **An action plan has to be set up immediately** in order to demonstrate that all these concerns will be addressed. In particular **the appointment of an independent Ombudsperson should be prioritized** and **the rules of procedure be further explained including by declassification**. **PCLOB members as well should be appointed**. **Those prioritized concerns need to be resolved by 25 May 2018**.

The WP29 expects **the remaining concerns to be addressed at the latest at the second joint review**.

In case no remedy is brought to the concerns of the WP29 in the given time frames, the members of WP29 will take appropriate action, including bringing the Privacy Shield Adequacy decision to national courts for them to make a reference to the CJEU for a preliminary ruling.

TABLE OF CONTENT

Introduction

On 6 October 2015[3], the European Court of Justice invalidated the Safe Harbor adequacy decision after having recalled the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the large number of persons whose fundamental rights are liable to be infringed where personal data is transferred to a third country not ensuring an adequate level of protection. Soon after, the Commission started negotiations for a new adequacy decision and presented a draft adequacy decision with its annexes.

On the 13 April 2016, the Working Party 29 issued an opinion[4] on the draft new adequacy decision aiming at replacing the invalidated Safe Harbor. On the same day, the WP29 also issued a working document[5] on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees).

On 12 July 2016, the European Commission adopted the EU-U.S. Privacy Shield adequacy decision[6] ("Privacy Shield"). The Privacy Shield entrusts the Commission with the task to assess the findings of the adequacy decision, including on the basis of the factual information collected in the context of an Annual Joint Review[7]. Important concerns on both the commercial aspects and aspects relating to government access to personal data transferred under the Privacy Shield for the purposes of Law Enforcement and National Security had then to be addressed and further assessed in the context of the Joint Review.

As also foreseen in recital 147, "*participation in this meeting will be open for EU DPAs and representatives of the Article 29 Working Party*".

The first Joint Review of the Privacy Shield took place on the 18 and 19 September 2017 in Washington DC. Eight representatives of the Article 29 Working Party, Commissioners as well as experts at staff level, were designated to be part of the WP29 Review Team ("the Review Team") that accompanied the Commission during this two-day meeting with U.S. authorities and companies.

In advance to the Joint Review, the Commission sent questionnaires to US companies adhering to the Privacy Shield and NGOs, as well as a detailed agenda to organize the discussions with the US authorities and stakeholders during the Joint Review itself. The WP 29 contributed to the elaboration of these documents.

The findings of this first Joint Review, stemming both from written submissions, as well as from oral contributions during the Joint Review itself, are presented in annex to this document. They were presented at the 3 and 4 October Plenary of the WP29.

On the basis of the fact-finding report, as well as on the basis of the previous opinions issued by the WP29, the Working Party with this paper has analyzed the concrete operation and enforcement of the Privacy Shield in order to assess the level of protection afforded to EU individuals when their data are transferred to the US under this framework.

---

[3] Case C-362/14

[4] WP 238

[5] WP 237

[6] 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.

[7] See recitals 145-149 and Article 4(4) of the decision.

I. On the commercial aspects of the Privacy Shield

A. Improvements brought by the Privacy Shield

During this first year of implementation of the Privacy Shield, the US authorities focused on the setting up of processes for the administration of the Privacy Shield program so as to enable companies to self-certify under the Privacy Shield and benefit from the program.

In this regard, the WP 29 **welcomes the various efforts made by US authorities to set up a comprehensive procedural framework to support the operation of the Privacy Shield**. The actions undertaken in this respect include the implementation of thorough procedural checks prior to the self-certification by a dedicated team within the Department of Commerce (DoC) in charge of administering the Privacy Shield program as well as specific steps taken for re-certification and for following up with companies that withdraw from the Privacy Shield list (see Annex).

Notwithstanding the improvements offered by the Privacy Shield compared to the Safe Harbor, the WP29 considers that **six series of concerns remain.**

B. Remaining concerns

1. Lack of guidance and information

1.1. Lack of guidance for the companies adhering to the Privacy Shield

The DoC published general guidance aimed at businesses notably through a Self-Certification Guide and Privacy Policy FAQs available on the Privacy Shield website. However, such guidance information mainly addresses procedural and organizational aspects and as indicated by the DoC remains purposely general on the substance of the requirements, to avoid overly prescriptive tools.

The DoC and the FTC stressed that the Privacy Shield is a principle-based self-certification system and that they privilege a case-by-case analysis of issues when they arise rather than through overly prescriptive guidance beforehand because they fear this could lead to organizations copy and paste recommended pieces of text without making it fit to the organizations' needs and therefore not complying with it.

While recognizing that the principle with a self-certification system is to give companies the responsibility to assess their compliance and in particular in the context of the Privacy Shield of their privacy policies with the Principles, the WP29 underlines that in turn, the companies should be in a position to do so correctly on the basis of a clear interpretation of how the substance of requirements set out under the Privacy Shield Principles are to be implemented in practice.

However, the WP 29 recalls that the Privacy Shield is a self-certification system which mainly relies on self-assessment, by the companies in the majority of cases[8], of their compliance with the principles of the Privacy Shield. Since 60% of the companies adhering to the Privacy Shield are SMEs,

[8] Only 17% of the companies use outside compliance review mechanisms.

and 83% of all companies adhering to the Privacy Shield conducted a self-assessment internally (and did not use the services of another company for an external compliance review), **clear guidance on the principles of the Privacy Shield appears indispensable**, both for the companies to correctly translate the requirements of the Privacy Shield in their privacy policies and for the individuals to exercise their rights to allow for an effective control over their data. While EU supervisory authorities remain available to exchange with the U.S. authorities as regards their respective interpretations of notions to ensure a common and coherent approach, especially to key concepts, the WP29 stresses that the respective responsibilities shall remain clear. Therefore, the U.S. authorities shall remain responsible for issuing guidance on the implementation of the Privacy Shield by U.S. companies adhering to the scheme, as they will then have the power to enforce the Privacy Shield.

More precise guidance should be provided with respect to the application of the Choice Principle on when and how a data subject can opt out from the processing of his/her data for a new purpose, and with respect to the application of the Notice Principle, and more specifically on the timing for certified organizations to give notice to individuals as stressed by the WP29 in its document WP238 on the adequacy of the draft Privacy Shield decision.

Concerning the requirements with regard to **onward transfers**, the DoC indicated that it had set up reminders for the companies before the end of the 9 months transitional period and provided feedback upon request to companies. However, it appeared that while this requirement was presented by all companies questioned as one of the most demanding to comply with, no general guidance was provided on this topic and the content of the updated contract clauses on these aspects was not checked by the US authorities.

Similarly, for the right of access, the Privacy Shield Supplemental Principles specify that access to personal data needs to be provided only to the extent that the Privacy Shield organization "*stores"* the personal information. While the WP29 positively notes that there is no indication as to a restrictive interpretation by the DoC of these provisions, limiting individuals' ability to access only to personal data that is *stored* by an organization, additional guidance to clarify this point would be welcomed.

1.2. Lack of clear and easily available information for EU individuals

The WP 29 recognizes that the information of EU individuals is primarily the responsibility of the European data protection authorities and the European Union institutions and Member States. To that end, the WP 29 and the national data protection authorities have notably published referral forms, set up of an EU centralized body and took part to awareness raising events. FAQs were also published to the attention of individuals regarding the Privacy Shield and their rights under this mechanism. In addition, several data protection authorities have hotline to answer specific questions addressed by EU individuals.

While doing so within the EU, the WP stresses that most of the information available on the Privacy Shield website is directed to the companies rather than to the individuals.

As stated in its previous opinion, the WP 29 recalls that in practice the various recourse procedures may prove to be too complex, difficult to use for EU individuals and therefore less effective.

In practice, as underlined by the companies providing independent recourse mechanisms (IRMs), most of the complaints are brought directly to the companies, in many cases, by individuals actually seeking general information on the Privacy Shield and the processing of their data.

Therefore, to complement the specific information provided in concrete cases by the companies themselves, the US authorities should strive to offer **more information in an accessible and easily understandable form to the individuals regarding their rights and available recourses and remedies.**

2. HR Data

A problem has shown up regarding the interpretation of the notion of **HR data**. Questioned on this notion, the DoC indicated that – like in Safe Harbor - only the processing of data of employees within the same company falls within the category of "HR data" under the Privacy Shield and benefits from the additional safeguards, notably the extended supervisory powers for the panel of EU DPAs, foreseen in this respect. As a consequence, processing of data of an EU company's employees after being transferred to a Privacy Shield certified processor within the US are not considered HR data but commercial data. The WP29, however, regards "HR data" as any personal data concerning an employee in the context of an employer-employee relationship. In the Joint Review it had emerged that there is a different reading of the notion "HR data" by the US government on one hand and the European Commission and the WP29 on the other side. It was always the expressed intention of the Commission to grant extra protection to HR data and expand the powers of DPAs in order to appropriately protect these data under the Privacy Shield through the EU DPAs informal panel that can give binding advice to certified organizations and as a last consequence refer the case to the FTC or ask the DoC to remove the organization not complying with such binding advice from the Privacy Shield list. This is also supported by the understanding of the term « HR data » in the Commission decision (EU) 1250/2016[9].

Consequently, the WP29 is of the opinion that any data concerning an employee in the context of an employer-employee relationship from an EU Company may only be transferred lawfully under the Privacy Shield if the receiving company has an active HR data certification.

The WP29 calls the European Commission to address this issue and, if necessary, engage in negotiations with the US authorities in order to amend the Privacy Shield mechanism accordingly.

3. Lack of oversight and supervision of compliance with the Principles

Privacy Shield brought significant improvements compared to Safe Harbor in terms of enhanced checks performed by the DoC prior to the listing of organizations and also with regard to the use of IRMs for outside compliance reviews for companies' Privacy Policies. However, the Privacy Shield is a system based on the concept of self-certification. Therefore it is of utmost importance that U.S. authorities involved in the administration of the Privacy Shield devote sufficient resources at

[9] Recital 48: "Organisations are obliged to cooperate in the investigation and the resolution of a complaint by a DPA either when it concerns the processing of human resources data collected in the context of an employment relationship (...)"; see also Recital 58: "cases where the organisation is either obliged to cooperate and comply with the advice of the DPAs as regards the processing of human resources data collected in the employment context (…)";

oversight and enforcement activities of the certified companies after the actual certification / recertification procedure. On the basis of the information collected during the Joint Review, it appears that the **oversight of the commercial aspects of the Privacy shield mainly relies on the third party companies providing Independent Recourse Mechanisms (IRMs)** and that the implementation of the Privacy Shield framework still lacks sufficient oversight and supervision of compliance in practice. The WP29 would also like to recall in this context that organizations having opted for external compliance review as part of their verification procedures have no obligation to provide training to their employees, or check that their policies are accurate, comprehensive, prominently displayed, implemented and accessible - as is the case for those having opted for internal review - and will only be subject to verification of compliance with their privacy policy by the third party organization.

With respect to the IRMs, the WP 29 noted that the companies providing these recourse mechanisms also offer outside compliance review services. The WP 29 welcomes the intention of the DoC to **harmonize the reports provided by the Independent Recourse Mechanisms (IRM)** and calls for an increased control over the companies providing such mechanisms. In particular, safeguards as regards the possible conflicts of interests which could arise when the same company provides both outside compliance review of the privacy policies *ex ante* and an independent recourse mechanism *ex post* for the same processing activities would be welcomed.

The Privacy Shield framework provides that the DoC will be conducting **periodic *ex officio* compliance reviews** to monitor on an ongoing basis the effective compliance of organizations with the framework.[10] However, at the time of the Joint Review no such compliance monitoring actions had been undertaken yet. The DoC also indicated that compliance questionnaires had been prepared and could be addressed to a company when it is suspected to be in breach of the Privacy Shield. As the DoC did not receive indication of any such suspicion, these questionnaires have only been used in a proactive way to help companies as regards their obligation on onward transfers.

In addition, the WP 29 notes that to date no **"sweep" specifically dedicated to Privacy Shield** companies or to specific requirements of the Privacy shield was conducted or even envisaged by the FTC. In particular it seems that the FTC only would consider such measures when they suspect that there might be a breach.

In the Schrems decision, the CJEU underlined the importance of effective detection and supervision mechanisms for the reliability of a system of self-certification.[11] The WP29 considers that the performance of compliance reviews of organizations having self-certified to the Privacy Shield is a key element for the effective functioning of the framework in order to identify any deficiencies and address them as appropriate even in the absence of suspicion of a company being non-compliant *a priori*.

In particular, the performance of such verifications once a company has certified to the Privacy Shield appear all the more important since as part of the self-certification, the DoC does not concretely check the content of the privacy policies of the companies when they submit an application for self-certification or whether these policies are concretely enforced within the companies. Also, as

[10] Annex I /Annex 1 (Letter from Acting Under Secretary for International Trade Ken Haytt) to Commission decision (EU) 1250/2016

[11] "(…) the reliability of such a system is founded essentially on the establishment of effective detection and supervision mechanisms enabling any infringements of the rules (…) to be identified and punished in practice" (CJEU, C-362/14 - Schrems, par. 81).

mentioned above, no checks have been carried out to date to assess whether the privacy provisions that are to be included by certified companies in contracts in case of onward transfers comply with the requirements of the Accountability for Onward Transfer Principle.

Therefore, even in the absence of complaints, such ex-officio **investigations have to be conducted both by the DoC and the FTC/DoT to ensure that self-certified organizations concretely implement the requirements of the Privacy Shield**, thus meeting the CJEU's requirement on an overall level of data protection.

WP29 hence believes that it is of utmost importance that the current supervision practice be broadened to routine monitoring by DoC and/or FTC for detecting false claims of participation in the Privacy Shield, in particular through internet searches, as well as to monitor – on an ongoing basis – effective compliance with the Privacy Shield principles by the certified companies. Possible elements for strengthening monitoring may include "sweeps" particularly dedicated to the Privacy Shield and the use of compliance questionnaires even without concrete suspicion of a breach of the Principles. However, other means of detecting cases of non-compliance, as e.g. on-site verifications, should be taken into consideration as well.

Therefore, as of now, monitoring of compliance with the Privacy Shield principles by the U.S. authorities involved (DoC, FTC and DoT) seems strongly focused on the certification and recertification process. After completion of the (re)certification procedure and in particular where no concrete suspicion of a breach has arisen, however, there appears to be a lack of oversight by the US authorities.

4. Application of the Privacy Shield to processors established in the US

While discussing the specific issue of HR data, it appeared that in the context of transfers under the Privacy Shield from a controller within the EU to a processor within the US, the purpose of the processing is considered to be for commercial purposes by the US authorities and the processing by the US company is considered to be distinct from the processing of the EU controller.

This **different interpretation concerning the processing activities of US processors imply various types of consequences**. For HR data, for instance, it implies that the US processor does not have the obligation to opt for the competence of the informal panel of EU DPAs.

More generally, this issue raises the question of the **control exercised over processors adhering to the Privacy Shield**. Indeed, while they should be bound by the provisions of the contract concluded with the EU controller, they will have to declare a different purpose for the processing when submitting an application to the DoC. As already stated in the previous opinion of the WP 29, several of the obligations included in the Principles are not suitable for data processors, as it is always the data controller that determines the purposes and means of the processing of the data. For this reason some obligations contained in the Principles, if applied to an organization acting as agent/processors, may contradict the data processing contract required under EU law. Therefore, the processor has no autonomy with respect to the processing of data. For example, the processor may not be authorized by the controller within the EU to onward transfer the data or only after the authorization of the controller within the EU. A processor would also not be able to provide individuals with full notice as intended by the Notice principle, for example because this organization does not determine the purposes of the processing. U.S. organizations receiving data for mere

processing purposes should also not be able to decide to process the data for their own purposes in order to respect the principle of purpose limitation.

In practice, the DoC confirmed that when examining a request for self-certification submitted by a company under the Privacy Shield, they do not differentiate between controllers and processors.

Although when the GDPR enters into force, many of these situations will fall directly under the scope of EU Law, the WP 29 calls on the US authorities to provide additional information concerning the specific situation of processors and to distinguish more clearly processors from controllers. This goes both when they apply for self-certification as well as when they are subject of checks to clarify which specific obligations apply to them and how.

5. Automated-decision making/Profiling

In its previous opinion, the WP 29 deplored the lack of guarantees in the Privacy Shield for automated decisions which produce legal effects or significantly affect the individual.

The necessity to provide for legal guarantees for automated decisions (producing legal effects or significantly affecting the individual) in order to provide an adequate level of protection has already been underlined by the WP29 in its Working Document 12.

The findings gathered during the Joint Review seem to indicate that none of the data transferred under the Privacy Shield are processed through automated decision making systems, and the information provided on the Fair Credit Reported Act confirm that specific rules exist under US Law in certain fields.

However the feedback from the companies remained very general, leaving unclear whether these assertions correspond to the reality of all companies adhering to the Privacy Shield, and these rules do not appear to cover all areas where automated decision making systems could be used given their very limited scope. **The WP29 calls upon the Commission to contemplate the possibility to provide for specific rules concerning automated decision making** to provide sufficient safeguards including the right to know the logic involved and to request reconsideration on a non-automated basis, especially after having explored the extent of the practical relevance of automated decision making processes by Privacy Shield certified companies if the analysis generates an actual need for additional safeguards.

6. Self-Certification Process and Cooperation between U.S. authorities in the Privacy Shield mechanism

A certification review process has been set up by the DoC to verify against the certification requirements the applications for self-certification submitted by companies wishing to adhere to the Privacy Shield and a system of regular reminders to companies before the expiry of their certification has been set-up with respect to the re-certification. However, the process as currently practiced seems to lead to some inconsistencies due to the fact that when a company submits its privacy policy to the DoC for completing the certification, the privacy policy - which needs to include a reference to the Privacy Shield certification – is already published on the company's website. Hence the company's website indicates a current Privacy Shield certification while the certification process has

not been completed yet and therefore the company has not yet been included on the Privacy Shield list on the DoC website.

As a rule, public statements made available on the EU-US Privacy Shield online list and the information published by US companies in their online Privacy Policies have to be consistent at all times. In practice however, companies should be encouraged to send "working links" to the DoC rather than separate documents of their privacy policies, as this would allow the companies to update these policies directly following the review by the DoC.

The WP29 welcomes the process set-up for managing the re-certification of companies and the provision of a specific deadline of one month from the end of a certification at the expiry of which a company which would have not recertified might be exposed to referral to the FTC while no deadline for recertification was provided under the Safe Harbor.

However, this procedure as currently practiced leads to an inconsistency between the actual certification status and the public indication on the Privacy Shield list of the DoC when a certification expires, since in this case the certification status is still indicated as active on the DoC list for as much as 30 days after the expiration. The WP29 underlines that there must be no gap in the protection of data received from the EU by the U.S. company during this one month period.

Considering both scenarios described, the WP29 considers that the DoC's recertification process must be adjusted in order to avoid a gap in the protection in particular for the data received either before the organization is being included on the DoC's list or after the expiration of the certification. The public statements made by the organizations in their privacy policies have to be synchronized with the publication on the Privacy Shield list flagging the organizations' certification as active. As soon as a certification has expired and the recertification process has not yet been completed, an organization's certification has to be flagged as inactive on the Privacy Shield list. If not so, this could create a risk of "false claims" situations for US participating companies.

In addition, procedures have been set up by the DoC and the Federal Trade Commission (FTC) to receive referrals and to exchange with the EU DPAs. Also the DoC has set up procedures with the FTC and the Department of Transportation (DoT) to determine which of them is competent over processing activities of a company wishing to submit an application to the Privacy shield scheme[12].

The WP29 regrets the absence, in practice, of proactive web search for false claims to concretely check the self-certified companies and the links made available to access their privacy policies. WP29 strongly suggests that the DoC and the FTC now focus their efforts to include such checks in their monitoring activity related to the Privacy Shield.

Furthermore, the WP 29 notes that no complaint from EU individuals was referred to the US authorities since the Privacy Shield has been established and welcomes the three enforcement actions undertaken by the FTC further to referrals from the DoC following complaints from persons located in the US. The WP 29 also awaits the final setting up of the arbitration panel which is announced to be operational by the end of the year.

In addition to the points mentioned above, the WP29 recalls remaining issues with respect to certain elements of the commercial part of the Privacy Shield adequacy decision as already raised in its

[12] See in annex for more details on these process.

Opinion 01/2016 in particular regarding the absence or the limitation to the rights of the data subjects (i.e. right to object, right to access, right to be informed for HR processing), the absence of key definitions, the lack of guarantees on transfers for regulatory purpose in the field of medical context and the overly broad exemption for publicly available information.

II. On the derogations to the Privacy Shield to allow access to data for Law Enforcement and National Security purposes

A. Improvements since the adoption of the Privacy Shield

The WP29 welcomes that the U.S. government has continued to publish a number of important documents, e.g. decisions by the Foreign Intelligence Surveillance Court[13] (FISA Court), in part by declassification. The publications and declassifications demonstrate the intention of the U.S. government and of the U.S. legislator to become more **transparent** about the use of surveillance powers. In addition, these documents help to better understand the working of the various surveillance programs, including the safeguards. The additional explanations and answers provided during the Joint Review also helped the WP29 to get a clearer understanding of these programs and safeguards and of their concrete impact on the level of data protection afforded.

The WP29 is also aware that the **surveillance laws in the U.S. are evolving**, both in part on the basis of new legislative proposals and new legislation, and also in part on the basis of more and more case law on surveillance matters.

Taking into account these developments as well as the findings of the Joint Review, some of the main points of concern for the WP29 expressed in previous opinions, in the area of access to data transferred under the Privacy Shield for national security or law enforcement purposes, have not been fully resolved. These **main concerns** are related to the collection of data, to oversight, to judicial redress and finally, to the Ombudsperson mechanism. This calls for a more detailed analysis:

B. Concerns

1. Collection of data (under section 702 and under EO 12333)

1.1. Collection of data for national security purposes under Section 702

In its Schrems judgment[14], the CJEU recalled that the "*protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary*"[15] and ruled that "*legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter*"[16].

In its previous opinion on the draft Privacy Shield decision[17], the WP29 recalled its long-standing position that *"massive and indiscriminate surveillance of individuals can never be considered as*

[13] U.S. federal court established and authorized under the Foreign Intelligence Surveillance Act of 1978 (FISA)
[14] Case C-362/14, 5 October 2015
[15] See recital 92, See also cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger, recital 52.
[16] See recital 94.
[17] See WP 238

proportionate and strictly necessary in a democratic society, as is required under the protection offered by the applicable fundamental rights".

During the Joint Review, in addition to the information already available in the PCLOB[18] report on section 702 of the Foreign Intelligence Surveillance Act (FISA), the U.S. government explained that **no bulk collection would take place inside the U.S.** and that collection of data in this context can only be based on FISA and the statutes related to National Security Letters. They confirmed that in every case only data of specific "targets" would be collected, after the tasking of a "selector" corresponding to this target (telephone, email address, etc). The U.S. authorities also stressed that the definition of "targets" and the tasking of selectors follow various internal checks and have to be in compliance with criteria approved by the FISA Court. The statistical transparency report of the Office of the Director of National Intelligence (ODNI) for 2016 shows the U.S. government issued orders for about 100.000 targets under section 702 of FISA.

Two programs are confirmed to be operating under Section 702 of FISA: PRISM and UPSTREAM.

Under both programs, the **definition of targets and the tasking of selectors** provided for in statute and the corresponding internal procedures and policies mention that U.S. signal intelligence activities under section 702 are "as tailored as feasible", as envisaged in the Presidential Policy Directive 28 (PPD 28)[19]. However no material evidence to demonstrate this, such as additional examples of categories of selectors, has been provided during the Joint Review.

In addition, it is important distinguish the two programs as regards access to data in order to apply selectors.

Under PRISM, the relevant U.S. authorities require internet service providers to provide them with the data of their users corresponding to "selectors", once "tasked" by the competent authority.

Under the UPSTREAM program[20], the providers of the telecommunication backbone are required to assist the NSA by identifying and collecting transiting data "to" and "from" a chosen "selector" in the flow of communications between communication service providers. As regards the latter program, although the WP29 welcomes the recent decision by the FISA court which resulted in the **termination of the "about" collection** in this context, and the oral assurances given by the U.S. authorities that this decision applies to all collection under section 702, regardless of the nationality, the WP29 notes that for the application of a selector to take place under the UPSTREAM program, **access to the flow of data** in itself seems to remain necessary. The WP29 still continues to recall its longstanding position on the risks involved with operating on the basis of this type of access, which, depending on the type of selectors used, could result in a massive collection of data.

The imminent decision **to re-authorize section 702 FISA** before the end of the year presents an important opportunity to include additional safeguards, such as enshrining the protections for non U.S. persons that are contained in PPD-28, and providing for precise targeting, along with the use of the criteria such as that of "reasonable suspicion"[21], to determine whether an individual or a group

[18] Privacy and Civil Liberties Oversight Board Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act JULY 2, 2014

[19] Presidential Policy Directive -- Signals Intelligence Activities, January 17, 2014

[20] See in Annex - the US representatives indicated that only 10% of the authorized interceptions under FISA are collected under the upstream program

[21] See Zakharov v. Russia, Application no. 47143/06, 4 December 2015 – par. 260

should be a target of surveillance, subject to approval of individual targets, subject to stricter scrutiny of individual targets by an independent authority ex-ante.

Consequently, on the basis of the information available and of the discussions during the Joint Review, the WP29 would need further evidence or legally binding commitments to substantiate the assertions by the U.S. authorities that the collection of data under section 702 is not indiscriminate and access is not conducted on a generalized basis under the UPSTREAM program.

The WP29 calls for further independent assessment on the necessity and proportionality of the definition of "targets" and of the tasking of selectors under section 702 (including in the context of the UPSTREAM program should it be maintained),as well as the concrete process of application of selectors in the context of the UPSTREAM program to clarify whether massive and indiscriminate access to data occur in the context of non-U.S. persons. The WP29 observes that the Privacy and Civil Liberties Oversight Board (PCLOB), as an independent oversight agency should be in a position to prepare and issue an updated report, building on the report issued in 2014.

1.2. Collection of data for national security purposes under Executive Order 12333

The WP29 is of the view that the analysis of the laws of the third-country for which adequacy is considered, should not be limited to the law and practice allowing for surveillance within that country's physical borders, but should also include an analysis of the legal grounds in that third country's law which enable it to conduct surveillance outside its territory as far as EU data are concerned. As already underlined in its previous opinion, "*it should be clear that the Privacy Shield Principles will apply from the moment the data transfer takes place*"[22], which means including as regards **data "on its way" to that country**. This is why the WP29, in the same opinion of last year, analysed the Executive Order 12333 and the Presidential Policy Directive 28 (PPD-28), which is all the more important in this context as it provides for the only safeguards and limits to the collection and use of data collected outside the U.S. as the limitations of FISA or other more specific U.S. law do not apply. During the Joint Review, the U.S. authorities underlined that Executive Order 12333 could not be used as a basis for collection of data inside the U.S. territory and that they consider that collection of data under this Executive Order falls outside the scope of the Privacy Shield. On several occasions, including during the Joint Review, they also recalled that information on the collection of data outside its territory for the purpose of national security can only be shared and published within limits.

The WP29 welcomes the adoption of PPD-28, as well as the commitment expressed by the current U.S. government and repeated during the Joint Review to comply with the rules set therein. Indeed, the PPD-28 provides limitations to the collection of data, as the signal intelligence activities have to be as "tailored as feasible", which have to be transposed in the internal policies of the relevant authorities.

However, no new information was provided during the Joint Review. In particular, no further information was provided during the Joint Review on the interpretation of PPD-28, especially on the six purposes allowing for the use of data foreseen in this text, nor on additional elements as to the amount of personal data collected in order to allow for a validation of the commitments and the assurances provided. Here again, given the uncertainty and unforseeability of how EO12333 is made use of, the PCLOB should be in a position to finish and issue its awaited report on EO 12 333 to

[22] See WP238

provide information on the concrete operation of this Executive order and on its necessity and proportionality with regard to interferences brought to data protection in this context.

2. Oversight

Comprehensive **oversight of all surveillance programs** is crucial, as the CJEU and the ECtHR have emphasized in many judgments.

The WP29 has been presented with the oversight activities of several entities and considers that a **comprehensive internal oversight structure**, independent from the Intelligence Community, is in place, including the Privacy and Civil Liberty officers, the oversight of the Department of Justice, and Inspector Generals, amongst others.

As expressed in its previous opinions, the WP29 is aware of the complex and multi-layered oversight structure established in the U.S. in order to ensure that personal data is collected and processed in accordance with U.S. law. By way of example, the WP29 is of the view that the offices of **the Inspector Generals**, institutions rarely known in most EU Member States, deserve credit for their work as a valuable check on the US government's agencies.

The WP29 stresses that it considers the **Privacy and Civil Liberties Oversight Board (PCLOB),** whose recommendations have been an important contribution to reforms in the U.S. and whose reports have been a particularly helpful source to understand the functioning of the various programs, as an independent body, to be an essential element of the oversight structure. It is therefore of utmost importance that the new members be appointed to the vacancies on the PCLOB as soon as possible. While the remaining and currently sole member of the PCLOB has given her assurance during the Joint Review that work is still ongoing, limitations to its ability to act and fulfill its obligations still continue. The WP29 understands that the current situation of the PCLOB is similar to other institutions and agencies during this transition period of the current US Administration. However, while a nomination of the new Chairman is pending, the WP 29 still recalls the necessity to ensure that the PCLOB will fully functional as soon as possible, in order to be able to finalize and issue its report on Executive Order 12 333 and to prepare and issue a new report on Section 702, in particular if it were to be reauthorized by the end of 2017. In addition, the WP29 regrets that the report on Presidential Policy Directive 28 (PPD28)[23] is still subject to Presidential privilege and is thus not published yet.

3. Redress for EU individuals

In its Schrems ruling, the CJEU has stressed the importance to have a right to an effective remedy before a tribunal[24]. In the understanding of the WP29, it follows that an adequacy finding of a third-country requires that an EU citizen must have access to an independent and impartial body, including in surveillance matters.

There was considerable discussion, during the Joint Review, but also in the different submissions to the Irish High court in the Schrems II case, about the availability of redress for EU citizens under the Administrative Procedure Act (APA) as well as under FISA. Whereas these statutes, APA and FISA,

[23] Presidential Policy Directive -- Signals Intelligence Activities – 17 January 2014

[24] See paragraph 95

appear to provide limited grounds for an EU individual to challenge surveillance in U.S. courts, the principal problem appears to concern the **"standing requirement"**.

As the U.S. government has repeatedly stated during the Joint Review, "standing" is a requirement under the U.S. constitution. According to the U.S. Supreme Court in Clapper v. Amnesty[25] , "standing" is "*the requirement that plaintiffs have sustained or will sustain direct injury or harm and that this harm is redressable*".[26] This admissibility threshold applies in surveillance cases, as the Supreme Court held in that decision. In addition, whereas notification is required in criminal proceedings, including for EU individuals, such obligation does not generally exist in surveillance matters. This distinction is important as the effective remedy required in view of Art. 47 of the Charter of Fundamental Rights and under the ECHR is not limited to cases of criminal law. Indeed, as underlined by the ECtHR in its leading case Zakharov[27], "*as soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should, however, be provided to the persons concerned*"[28].

During the Joint Review, the WP29 representatives have also been confronted with case law from courts in the Member States of the European Union, which have also denied challenges to surveillance laws of the Member States for procedural reasons similar to the doctrine of "standing". Although the WP29 notes that concern, it underlines that the relevant criteria to take into account concerning the assessment of adequacy are those stemming from the jurisprudence of the highest courts in Europe, meaning the CJEU and ECtHR. In addition to the CJEU in Schrems, the ECtHR in Zakharov has also outlined its flexible approach focused more on the protection of individuals' personal data with the aim to *"ensure that the secrecy of surveillance measures does not result in the measures being effectively unchallengeable and outside the national judicial authorities and of the Court."*[29]

Under the procedural requirements as currently interpreted by the U.S. courts, it appears to be difficult and uncertain that an EU individual could satisfy the procedural requirement of standing when bringing a suit against a surveillance measure on the basis of section 702 FISA or EO 12333. The WP29 will therefore continue to follow closely the evolution of these cases as they could provide additional guarantees concerning the effectiveness of judicial redress offered before U.S. courts. However, as was confirmed during the Joint Review, the interpretation of the notion of "standing" in surveillance matters is evolving with cases pending[30].

4. Ombudsperson mechanism

Since the effective remedy before an independent tribunal is of such importance in the jurisprudence of the European courts, the WP29 welcomed the establishment of an **Ombudsperson** mechanism as a new redress mechanism in its previous opinion. It underlined that this may constitute a significant improvement for EU individuals' rights with regards to U.S. intelligence activities. The Ombudsperson mechanism complements the possibilities of redress, or more critically, it might be argued that it is

[25] Clapper v. Amnesty International, 568 U.S. 398 (2013)
[26] "the requirement that plaintiffs have sustained or will sustain direct injury or harm and that this harm is redressable. At the Federal level, legal actions cannot be brought simply on the ground that an individual or group is displeased with a government action or law." Clapper v. Amnesty International USA
[27] Zakharov v. Russia, Application no. 47143/06, 4 December 2015.
[28] Zakharov, 287
[29] Zakharov, 171.
[30] See in particular cases ACLU v. Clapper, and Wikimedia v. NSA

meant to compensate for the uncertainty or unlikeliness to seek effective redress before a U.S. court in surveillance matters. In addition, as the PPD-28 does not create rights, it appears that the individual cannot go to court based on an alleged violation of the PPD-28. Thus, the only way for EU individuals to ask for a verification that the relevant authorities have complied with the requirements of this instrument is to ask the Ombudsperson to refer the matter to the competent Inspector General to check the internal policies of these authorities.

With Art. 47 of the Charter of Fundamental Rights in mind, the threshold of independence and impartiality required in a redress mechanism is high for the Ombudsperson. When assessing the Ombudsperson mechanism in its opinion of last year, the WP29 suggested that the appointment of a high-ranking official in the Department of State as the Ombudsperson is problematic, but may not necessarily lead to the conclusion that she is not sufficiently independent in the meaning of Art. 47. Having analysed the jurisprudence of the ECtHR in particular, the WP29 favored an approach which took into account the powers of the Ombudsperson, in particular the powers to access information as well as to remedy non-compliance.

During the Joint Review, the U.S. government explained in some detail the important work done in order to ensure that requests would be handled lawfully and efficiently. The acting Ombudsperson also stressed that she needs to be convinced of the findings before responding to the request. While the WP29 has no reason whatsoever to doubt the integrity of the (acting) Ombudsperson, in line with its previous approach, it recalls that a permanent Ombudsperson should be appointed as soon as possible as well as its expectation to learn more about the powers that the Ombudsperson has vis-à-vis the Intelligence Community. This information however was only partially shared after the Joint Review. The procedures governing the access to relevant information by the Ombudsperson and governing the interactions of the Ombudsperson with the other members of the Intelligence Community, including the oversight bodies, remain classified. Only examples illustrating how cases would be handled were shared with the WP29 after the Joint Review. Nevertheless, as long as the applicable procedures will remain classified and will not be shared, the WP29 will not be in a position to assess whether the Ombudsperson is vested with sufficient powers to access information and to remedy non-compliance.

Based on the available information, the WP29 doubts that the powers to remedy non-compliance vis-à-vis the intelligence authorities are sufficient, as the “power” of the Ombudsperson seems to be limited to decide not to confirm compliance towards the petitioner. As the WP29 understands, she is not vested with powers, which courts or other similarly independent bodies would usually be granted to fulfil their role. Therefore, the WP29 is not in position to hold that the Ombudsperson is vested with adequate powers to effectively exercise its duty. In addition, it was confirmed during the Joint Review that the decisions of the Ombudsperson cannot be brought to court.

The WP 29 recalls the lack of judicial review of the decisions of the Ombudsperson and consequently the impossibility to obtain remedies where the Ombudsperson will not provide any answer. The WP 29 is therefore not yet in a position to hold that the Ombudsperson can be considered an “effective remedy before a tribunal” in the meaning of Art. 47 of the Charter of Fundamental Rights.

5. Access to data for law enforcement purposes

As regards **access to data for law enforcement purposes**, the WP29 notes that the procedural safeguards inherent to the criminal procedure seem to imply that data are accessed for a specific purpose and that individuals are notified that their data have been accessed within the framework of criminal proceedings, in the context of which they can have access to judicial redress. However, it

recalls its concerns as regards effective remedies available to individuals in cases where the data of companies will have been accessed by law enforcement authorities, as underlined in its previous opinion[31].

Conclusion

The WP29 acknowledges the **progress of the Privacy Shield in comparison with the invalidated Safe Harbor Decision**. The WP29 recognizes the efforts made by the U.S. authorities and the Commission to implement the Privacy Shield. To complement these efforts, the WP29 will engage in advising the U.S. authorities in drafting new guidance, in particular regarding HR data and onward transfers, in order to develop a common understanding of the Privacy Shield Principles and to address the needs of the business community on both sides of the Atlantic.

However, **the WP29 has identified a number of significant concerns that need to be addressed by both the Commission and the U.S. authorities**. **Therefore the WP29 calls upon the Commission and the U.S. competent authorities to restart discussions**. **An action plan has to be set up immediately** in order to demonstrate that all these concerns will be addressed. In particular **the appointment of an independent Ombudsperson should be prioritized** and **the rules of procedure be further explained including by declassification**. **PCLOB members as well should be appointed**. **Those prioritized concerns need to be resolved by 25 May 2018**.

The WP29 expects **the remaining concerns to be addressed at the latest at the second joint review**.

In case no remedy is brought to the concerns of the WP29 in the given time frames, the members of WP29 will take appropriate action, including bringing the Privacy Shield Adequacy decision to national courts for them to make a reference to the CJEU for a preliminary ruling.

[31] WP 238

Annex – Facts collected during the Joint Review

As foreseen in the Privacy Shield Decision of 12 July 2016[32], the accuracy of the findings in this adequacy decision have to be verified by the European Commission, including on the basis of the factual findings in the context of an Annual Joint Review[33].

The first annual Joint Review took place on the 18 and 19 September 2017 in Washington.

8 representatives of the Article 29 Working Party accompanied the Commission during this two-day meeting with U.S. authorities and companies. Both the commercial aspects and aspects relating to government access to personal data were discussed.

These findings are presented hereafter in order to allow the WP29 to evaluate the adequacy of the Privacy Shield decision as well as the enforcement of this decision.

1. Program Implementation by the Department of Commerce (DoC)

1.1 Figures

Over 2 400 organizations are self-certified under the Privacy Shield, among which **60% are SMEs**. 1 590 self-certified during the first two months, and about 20 new applications arrive each week. The DoC stated that more companies had self-certified under the Privacy Shield than in the first 10 years of the Safe Harbor scheme.

To date, **150 companies recertified**, **1 failed to recertify** and **10 withdrew** (among which 6 returned or deleted the data, 3 kept the data while applying adequate protection and 1 keeps applying the Privacy Shield principles to these data). Reasons for withdrawal included merger with another company and the fact that some companies were no longer in business.

While 2 492 companies finalized their self-certification, 404 received requirements to take action following the initial review of their policies, and 78 are awaiting initial review.

Questioned on the existence of cases where self-certifications submitted were rejected, the DoC indicated that to date this situation did not occur.

1.2 Verification of the self-certifications submitted

The DoC presented the team working on the Privacy Shield (10 persons – each one following his or her files completely, from the beginning to the end), and dwelled on the procedures set up to check and verify the self-certifications submitted by the companies under the Privacy Shield scheme.

[32] 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.

[33] See recitals 145-149 and Article 4(4) of the decision.

The DoC underlined that when submitting their application for self-certification formally through the website of the Privacy Shield, the companies enter the final stage (meaning they undertook the preparation of their internal policies in advance).

Regarding the **method of verification by the companies themselves** that their claims to apply the Privacy Shield principles are effective before submitting their application, the DoC indicated that there are two ways to do so: self-assessment or outside compliance review by a third-party. 83% of the companies conducted a self-assessment internally before applying for the self-certification, while 17% turned to an outside compliance review.

The representatives of Hunton and Williams and Microsoft also confirmed that they had extensive exchanges with the DoC when reviewing and modifying their privacy policies in a very collaborative spirit.

As regards the **review of the applications submitted by the companies to the DoC**, the representatives of the DoC indicated that the initial review is led within 2 weeks after the submission and that they set up a 45-day requirement to complete self-certification process, and elaborated a standardized communication with companies. The privacy policies submitted are checked against 13 criteria.

Additional information received after the Joint Review:

- *Clarification on the 45-day period within which companies have to complete their self-certification process*
  The 45-day period begins the day on which the DoC raises issues in the context of the review process.

The verification of the applications by the DoC comprises **many procedural checks** (indication of the name and address of the company, contact details of a corporate officer responsible for the Privacy Shield compliance, characteristics of the organization and annual revenue, in order to calculate the fee to be part of the Program, indication of the type of data processed – Human Resources (HR)/non HR – as well as designation of all covered entities and indication of the dispute resolution mechanism chosen when the data processed are not HR data).

Eventually, companies also have to indicate under the jurisdiction of which authority their activity falls – US Department of Transportation (DoT) or FTC – which is a requirement for joining the Shield and makes enforcement of the self-certification binding, and to submit their privacy policies and give the website link to these policies in order to ensure that they are made publicly available).

The amount of the fee to pay is smaller for small companies and higher for bigger companies. This fee is used to self-fund the DoC's work on the Shield.

The DoC indicated that during the majority of self-certification reviews, the Privacy Shield team has to ask the self-certifying organization to **provide additional information or address deficiencies** before the self-certification can be finalized.

The majority of requests made by the DoC concern the imprecise description of the purposes of the processing, and situations where the Independent Recourse Mechanism provider mentioned

in the policies has not yet been engaged by the company (which appears at the time the DoC proactively contacts the IRM to check with it).

Some **typical deficiencies found in Privacy Shield applications** are the obligation to notify whether the company is doing onward transfers or not, as well as the liability related to such onward transfers. According to the DoC, typical errors of the early days (for example, companies referencing to Safe Harbor in their privacy policy or the listing of European entities) might not be seen as much as before.

The DoC also indicated that entities or subsidiaries of a same company could have different purposes for the processing which imply in this case different privacy policies to be submitted for self-certification.

Questioned on the **level of details of the checks** in general and with an example of a company that states that the right to opt out could be exercised by browser settings, the DoC indicated it would check, especially as regards the issue of browser settings.

Questioned on the self-certification review, the DoC indicated that they do not differentiate policies from controllers or from processors when examining them.

1.3 Recertification

As regards the **process for recertification**, the DoC indicated that regular reminders are sent to the companies before their self-certification expiry date (30 days, then 2 weeks and one day in advance before expiry). After the recertification date, the same process as for initial self-certification review starts again. When companies do not recertify, they automatically lapse and appear on the inactive list after 30 days (this extra month is foreseen for companies engaged in the process of recertification). Companies have in addition the obligation to withdraw (actively), which explains why the questionnaires include the question if the companies would like to withdraw. If the companies do not reply within 30 days, they might expose themselves to a referral procedure to the FTC for potential action.

Questioned on the one-month-delay during which companies remain on the list while they have not yet recertified, the DoC indicated that it was meant to allow companies to bring their policies in conformity.

1.4 Accessibility of the privacy policies of the companies

If the company is processing non-HR data, the privacy policy has to be publicly available (the company must provide a link to the webpage where its privacy policy is accessible). If HR data are processed, the privacy policy is not required to be publicly available, but the company must indicate to employees where the document is available.

Questioned on the accessibility of the policies of the companies, the DoC indicated they checked the links sent by the companies, but the representatives present needed to check if the availability of the policies on the websites of the companies was also verified. The DoC does not check the positioning of the privacy policy links on the company websites e.g whether they are available on the home page. The DoC uses crawlers to identify dead links to the Privacy policies on their website about once a month.

1.5 List of the self- companies

To the question to know whether the list indicates that a company's self-certification is currently ongoing, the DoC replied that the Privacy Shield **list contains only companies with a finalized self-certification**. This issue would be solved by the false claims referral procedure.

Questioned on **inactive or faulty links**, the DoC asked for screenshots or any feedback to tackle the issue. It also underlined that when looking for a company or a subsidiary, one shouldn't press "enter" to get the list of results.

Questioned on the differences and sometimes the discrepancy between the purpose indicated on the Privacy Shield website and the policies of the companies, the DoC indicated that there is a high level of subjectivity on this issue. On this issue as well as on the follow-up of the requirement to opt-out for companies the DoC indicated they would come back.

To a question on whether companies could already use the Privacy Shield logo during the 45 days delay, the DoC answered that in order to submit a self-certification, a company has to provide a privacy policy making reference to the privacy shield program which has to be publicly available (for non-HR data transfers).

1.6 Tools developed by the DoC to monitor the compliance of companies (compliance questionnaires, FAQs, guidance)

The DoC indicated that they have developed tools to monitor the compliance of the self-certifications, through **compliance questionnaires**, inquiries from the companies (mainly on onward transfers, enforcement authority jurisdiction and covered entities) and Privacy Shield Record Scans of the accessibility of Privacy Policies. Draft copies of the questionnaires were made available to before the review meeting.

On a question aiming to know in which instances the DoC would make use of compliance questionnaires, the DoC answered that these questionnaires are used when a company is suspected to be in breach of the Privacy Shield. However, these have not been used as of today because the DoC did not receive indication that a company was suspicious. For companies in the 9-months transition period, questionnaires were used as a proactive tool.

To a question on **FAQs** and the intention of developing more guidance, the DoC replied it had issued Privacy Policies' FAQs, but had not issued guidance on substance, and that they wanted to avoid the "one-size-fits-all" solution. DoC stated that the Shield is a principles based system and they do not want to provide overly prescriptive **guidance**. They therefore privilege case-by-case analysis and do not foresee any further guidance or FAQs so far. Most recent guidance would be on the arbitration mechanism. Generally guidance is triggered by issues raising from real life experience with the Companies.

1.7 Program assessment of the DoC

The DoC also presented its program assessment which aims at identifying common challenges faced by self-certified companies, developing guidance for team's use or website dissemination, ensuring consistent application of the requirements and assessing the website functionality and addressing any issues arising. The Privacy Shield team has weekly meetings and ad hoc discussions when issues arise.

1.8 Oversight

As regards the oversight, the DoC underlined their cooperation with the FTC (referrals are possible, as well as investigatory support provided to the FTC upon request).

The FTC mentioned that the **DoC referred 11 companies**, which stated to participate but did not finalize their self-certification. The FTC did not however take action against all of these companies, as some dropped out and others came into compliance very soon after the referral.

The DoC also presented its **proactive outreach**, including to remind companies of the forthcoming end of the transitional period for onward transfers.

1.9 False claims

On the issue of false claims, the DoC underlined that the **45-day delay has been set up to complete the self-certification process**, as well as the warning letters sent from the Office of the General Counsel. However, questioned on this, they confirmed that during this 45-day period, the company submitting its policies refers to the Privacy Shield in it and provides public access to these policies to comply with the requirements of the Privacy Shield, while it is not yet self-certified.

Questioned on other actions (like **web-searches**) against companies using wrongly the "Privacy Shield seal", to prevent false claims, without having submitted a request for self-certification, the DoC indicated that they had not undertaken such actions.

Questioned on the **remedies for false claims**, the FTC indicated that in some cases they publish reports, sometimes they lead privacy review programs, and in some cases they prepare settlement agreements (in which case comments on the sanctions proposed are possible, but in practice almost never upheld). It confirmed that the eligibility for complaints does not include the criteria of residence.

1.10 Redress mechanisms

On the **redress mechanisms**, the DoC recalled that the Privacy Shield list offers contact details for each self-certified company, contact details of the elected independent recourse mechanism, referrals to the DoC and the binding arbitration mechanism.

For US Privacy Shield companies receiving HR Data from the EU (33%) the redress mechanism is provided by the panel of EU DPAs. For the rest, they have an option to choose either the EU panel of DPAs or an Independent Recourse Mechanisms providers (IRMs).

As regards **complaints**, the DoC underlined that many, if not all, complaints were addressed directly to the companies. As regards the complaints handled by the DoC and referred to the FTC, no complaint has been referred yet despite the referral form published and the compliance questionnaire.

1.11 Specific issues

1.11.1 Onward transfers

Questioned on onward transfers, the DoC indicated that companies have to update their terms of service and/or contracts with processors but that they did not check if the companies brought their contract in conformity. They engaged in consultations on contractual terms upon request of the companies, and provided advice when asked.

All representatives of companies consulted underlined that the most difficult requirement to comply with concerns the onward transfers as it implied the re-negotiation of the contracts (which in some cases resulted in the termination of some contracts).

1.11.2 HR Data

The DoC indicated that they have issued **guidelines** to indicate that only data of a company's own employees are covered. In these cases EU employment law remains however applicable. They confirmed that in situations where a processor in the US processes data of an for an EU company and of this EU company's employees, the processing is considered to be of customers or clients data and falls out of the HR data rules of the Privacy Shield.

This confirmed that there is clearly a **different interpretation of what the notion of HR-data should cover**. The FTC explained that in any case, there is no jurisdiction gap. However, the fact that US service providers processing HR-Data are actually considered by the DoC as processing customer data has a direct impact on the type of dispute resolution mechanism, as in such case the panel of EU DPAs would not be competent. The DoC stated that they will endeavor to clarify on their website what they are talking about when they are referring to HR Data.

To a question on **limits to FTC jurisdiction on HR Data**, the FTC confirmed that, as addressed by a letter during the Safe Harbor negotiations, its jurisdiction is not excluded from HR Data processing carried out by companies belonging to an activity sector normally not falling under its jurisdiction. For example, HR data processing carried out by a pharmacy company falls under FTC jurisdiction.

To a question aiming to know whom to address (FTC or Doc) in case of a **violation**, the DoC answered that such cases can be sent to the DoC, with the possibility of referral to the FTC in case the company does not cooperate.

On a question on whether the FTC conducted any **on-site inspections of such processing**, the FTC answered that companies are taking a commitment to cooperate with the panel of EU DPAs. If they do not, this would constitute a "persistent failure to comply". The DoC explained that the US participating company has to provide a statement. In case EU DPAs have a doubt that the US company is complying with the Privacy Shield, this can be notified to the DoC and the company might be delisted.

On **aggregated HR data, exemption of notice/choice for HR data, on sensitiveness of HR data**, the DoC indicated that they had no knowledge of such cases, but will check if they find

examples and come back to us on this. Nothing has been received yet on these points. However, the DoC shared after the review its internal guidelines used on a day-to-day basis by the Privacy Shield team, which does not contain further explanations on HR Data.

1.11.3 Automated decisions

The FTC gave a presentation of the **Fair Credit Reporting Act (FCRA)** and of enforcement cases (Instant Checkmate, Spokeo, Certegy and Telecheck) under the FCRA. However, none of the US credit reporting agency is actually Privacy Shield self-certified and it remained unclear to what extent the FCRA is relevant in the context of a Privacy Shield transfer of personal data from the EU, as it would most probably apply only in a purely US context.

On a question on whether behavioral advertising processing falls in the scope of the FCRA, the FTC answered that the FCRA does not apply to marketing activities, except for pre-screen insurance processing.

In addition, under the FCRA each person is entitled to make an access request free of charge with each of the credit reporting agencies (CRAs), however further requests will – except for special cases – not be free of charge.

The FTC also presented the **Equal Credit Opportunity Act (ECOA)**, which entitles clients with some transparency rights as well as rights against discrimination (based on race, color, origin, etc.). However, this act would apply only to lenders and not to Privacy Shield self-certified companies.

The FTC admitted struggling to find an example. The FCRA dates back to 1970 and has evolved many times since. For example, it applies to employment background checks and housing decisions, not only to credit agencies. Apart from credit reporting agencies, other entities could fall into the scope of the FCRA, which will apply whenever data are used for certain specific purposes. The COM asked to see more evidence on this point.

As regards automated decision making, the companies indicated that there are specific laws to limit the use of profiles, such as the Fair Credit Reporting Act[34]. All four companies stated that automated decisions-making was not part of their business models, nor of their clients' business models.

2. Independent Recourse Mechanisms

The DoC indicated that discussions were ongoing to **standardize the annual reporting of the IRMs**, as the work is still in progress to adjust.

The "Better Business Bureaus" (BBB) and of TrustE (a subsidiary of TrustArc) presented their activities and indicated that they offered outside compliance review services as well as independent dispute resolution mechanisms.

[34] 15 U.S.C. § 1681

Questioned on this, the IRMs confirmed that the individuals do not have the obligation to go first to the company to seize them.

On the notion of "**eligible complaint**", they indicated that they had to concern data collected in the EU, transferred to the US under the Privacy Shield, and a complaint concerning a violation.

They also indicated that in many cases persons do not know what to do and therefore file a complaint. While most of the cases are brought by individuals, some are brought by academics or associations, who file more technical complaints.

Questioned on the **suspension of the "seal"**, they indicated that they would discuss with the DoC about the suspension of the seal in case of non-compliance but that it never happened – due to the lack of cases that needed escalation.

The DoC confirmed that a **persistent failure to comply** could be triggered in a case of a company not complying with a determination of the IRM.

Questioned on the **binding nature of IRMs dispute resolutions for parties**, they confirmed that their decisions are not binding on individuals who may pursue all additional Privacy Shield remedies.

Questioned on the **possible conflicts of interests for IRMs leading both outside compliance review and offering dispute resolution mechanisms**, they ensured that these activities are led by two distinct divisions in the company, that they work with a law firm if necessary, and that they review the compliance of the company with its policies. They confirmed that evidence from verification could inform the dispute resolution process and that they would kick a non-complying company out of the list.

Concerning **the compliance review**, they indicated that they check *in concreto* the policies and contracts of the companies, and that as the mechanism relies on self-assessment, companies keep records for investigations.

A question aiming to obtain more information about **pending complaints** mentioned in some IRM's annual reports (TRUSTe, BBB) was asked during the review (status, type of complaints). The IRM said they will check and come back.

Additional information received after the Joint Review:

- *<u>On the state of play of the pending complaints with IRMs</u> (situation on 25 September 2017):*
    - *Supplemental Complaint Information from BBB: In the BBB EU Privacy Shield Annual Procedure Report, a single complaint was identified as still pending at the end of the review period. The complaint form was submitted July 25, 2017 by an individual in Hungary, identifying a business participating in our program. The complaints field in the online form did not state a complaint and in fact contained only a single word. We sent a response to the complainant in English and in the Hungarian language, describing our*

privacy complaint handling service and requesting additional information to support a privacy complaint. We have received no further information from the complainant, and the complaint has now been closed as ineligible.

- *Supplemental Complaint Information from TRUSTe: The current status of the pending cases in our report are as follows: As of the 31st of July, there were 4 pending cases. Three of those cases related solely to companies participating in the EU-US Privacy Shield. One of those cases related to a participant in both the EU-US Privacy Shield and the Swiss-US Privacy Shield. While all 4 cases have progressed since the date of our report, all 4 remain pending, however, one of the cases in the EU-US Privacy Shield category is very close to final resolution. Substantively, two of the pending cases fall into the type of complaint category we call, "Unable to Change/Remove Personal Information," one of the pending cases relates to help with features and functionality, and one of the pending cases relates to abuse by another user.*

- *Number of companies that had DPAs as their IRMs (as of 3 October 2017):*
  - *223 organizations use DPA for HR and non-HR*
  - *232 organizations use DPA for non-HR only*

3. Enforcement activities of the Department of Transportation and of the Federal Trade Commission

3.1 Department of Transportation

The **DoT** made a presentation of its jurisdiction (over airline agencies and ticket agencies on the basis of the Unfair and deceptive practices Act) and of its activities.

It has the authority to enforce civil penalties (up to 22 100 dollars for each violation).

No airline company currently adheres to the Privacy Shield, and initially 27 entities identified DoT as regulator (some by mistake). In total, **13** Privacy Shield **companies are registered under the DoT's jurisdiction** . Ffor 10 of them, DoT's jurisdiction has been validated, while the jurisdiction issue of the other 3 is being examined. All of these 3 companies nevertheless appear on the Privacy Shield list.

Questioned on this, the DoT, the DoC and the FTC indicated that the allocation of jurisdiction between the DoT and the FTC did not stop the self-certification process as the DoT and the FTC have concurrent jurisdiction. Therefore, in any case, the FTC would have jurisdiction if the DoT does not.

Additional information received after the Joint Review:

- *Clarification of Information Regarding Participants that Indicated DoT Jurisdiction*
  As of 21 September 2017, 13 organizations on the Privacy Shield List have indicated in their Privacy Shield records that they are subject to Department of Transportation jurisdiction. The team has confirmed with 10 organizations that they are subject to DoT jurisdiction and is still waiting to hear back from 3.

3.2 Federal Trade Commission

The **FTC** made a presentation of its **enforcement powers**, illustrated with cases, which did not concern the Privacy Shield. On the three cases opened recently, which concern the Privacy Shield, the FTC underlined that blog posts were published for each new case. The FTC also indicated that they search their complaints database every month for Privacy Shield complaints.

Questioned on the **3 cases of complaints brought before the FTC**, the FTC indicated that they all stem from persons located in the US:

- 1 concerns a privacy policy notice to which someone objected as if it were a spam;
- 1 concerns privacy policies sent to the FTC with highlighted paragraphs without any further explanations or requests;
- 1 concerns a company which did not self-certify under the Privacy Shield.

Further questioned on this, the FTC confirmed that all **complaints** brought concerned US persons in the US. The FTC also underlined that complaints brought before the FTC did not concern the Privacy Shield at the beginning.

As regards the **situations triggering the enforcement actions of the FTC**, its representatives indicated that in some cases claims are made, in others the FTC does its own testing through sweeps, and sometimes cases are opened on the basis of information coming from the press. In addition, the FTC underlined that they coordinate their actions with other authorities, including from other countries.

Questioned on the possibility and probability to conduct a **sweep specifically on the Privacy Shield**, the FTC indicated that they could but that any concern under the Privacy Shield would be assessed as a deceptive practice action under section 5. If they did, they would do a sweep on certain issues of the Privacy Shield, as they undertake controls only when they suspect that there is an issue ("reason to believe"). The FTC also indicated that it has corrective powers (to ask for the deletion of data, or for corrective information of the consumers for instance).

As regards the **referral**, the FTC indicated that the forms are published since last July, that referrals are not treated as confidential (to allow for a discussion between the FTC and the EU DPAs) and that an email address has been created. Questioned on the mandatory elements if the referrals, the FTC underlined that the more information received, the easier it was to process the referrals.

4. Arbitral Administration and the Binding Arbitration Mechanism.

The DoC gave updates on the selection of the panel (the new deadline to select the last 4 members missing is 6 October 2017).

The representatives of the "American Arbitration Association" ("Triple A") presented their activities and the team dedicated to the Privacy Shield.

Questioned on the notion of "unjustified or disproportionate costs", Triple A indicated that it could imply a limitation on the documents to translate in order to limit the costs, and that there would be a case-by-case evaluation.

5. Legal developments relevant for the commercial aspects

The FTC mentioned two legal developments:

1. A change in some FCC rules about entities covered by the FCC jurisdiction but this does not change the Privacy Shield directly;
2. A court case currently pending addressing jurisdiction issues between the FTC and the FCC (FTC v. AT&T) around the question of whether a "common carrier" has a statutory or an activity exemption. The case is being appealed. In any case, this may affect the size of the Shield (some companies might not be able to joint anymore because they might not fall under the jurisdiction of the FTC anymore) but this is no affecting the strength of the Shield.

*
* *

6. Government Access to data in the field of Law enforcement and National Security.

6.1 Transparency

The representatives recalled that **all texts are public**, but that the intelligence community (IC) operates in secret. The balance between the necessary secrecy and the necessary transparency is difficult to find, and that a fully transparent IC would be fully inefficient. They also recalled that the US IC relies on multiple players with multiple layers of oversight.

They underlined that the Congress has "the power of the purse" and that reports of the Intelligence Oversight Board (part of the President's Intelligence Advisory Board, within the executive branch) are important.

On the public transparency, they indicated that there are **four principles of Intelligence Transparency**:
- What?
- How?
- Protection of classified information when necessary
- "Just do it" principle.

Concretely, they indicated that they check every word when releasing documents, to ensure that redactions are challenged, which is expensive, and implies also crosschecks of what is already public.

They also underlined that **transparency is a matter of Federal Law**, with the Freedom of Information Act[35] (FOIA) and the USA Freedom Act[36].

6.2 Collection/Access

6.2.1 Law Enforcement access

About **Law Enforcement access**, one form comes from the Wiretap Act and relies on court's orders and minimization principle. Data must be handled carefully.

6.2.2 Section 215

In the field of **Intelligence**, the authority under **section 215** has been significantly amended in the USA Freedom Act.

The authorities indicated that FISA Court now has to allow amicus standing due to the amendment of the USA Freedom Act in section 215 proceedings.

The discussion focused on access to data transferred to the US under the Privacy Shield and already in the US.

6.2.3 Section 702 of FISA

On the basis of the **Foreign Intelligence Surveillance Act (FISA)**[37], any demand to a US company must be done under the relevant statute, all of which would require "targeted requests" while prohibiting "bulk collection", regardless of nationality. This means that a specific "selector" is requested.

Questioned on **section 702 of FISA**, the US representatives underlined that it is **not a bulk collection program** and that it implies "targets", while bulk collection is essentially done overseas under another act than Section 702. On the territory on the US, collection of personal data are made on the basis of FISA or of the National Security letters Statute, which either prohibit bulk collection or explicitly obliges to have targeted selection.

Questioned on what a **"selector"** is, they indicated that they have not found a way of being more specific. They recalled that it could be an email address. The number of persons targeted under Section 702 would be close to 100.000 by now.

Questioned on the **use of selectors** in the context of upstream collection under section 702 of FISA, the US representatives indicated that only 10% of the authorized interceptions under FISA are collected under the upstream program e. They also confirmed that the court examines and approves

[35] 5 U.S.C. § 552

36 USA FREEDOM Act of 2015, Pub. L. No 114-23

[37] 50 U.S. Code Chapter 36 - FOREIGN INTELLIGENCE SURVEILLANCE

(by way of certification) the targeting procedure under 702, but does not approve of the individual targets before they are applied ("ex-ante").

The US representatives also recalled the recent case before the FISC which resulted in the **termination of the "about collection"** in the context of upstream programs. Concretely, they explained that while before all the data about a target were collected (which means also, for instance, emails mentioning the target), this decision results in the collection of data only from or to the target. Initially focused on US citizens, this decision applies to all collection under section 702, regardless of the nationality. No statistics or figures are available on the amount of data not collected with the end of "about collection".

Questioned on the **protection granted to EU citizens under section 702**, the US representatives pointed to the purpose of the collection under section 702, which would be limited to obtain "foreign intelligence information", as further defined in FISA and in the certifications sought from the FISC. In addition, non-US citizens would also benefit from the agencies' retention and minimization procedures, at least as a matter of practice.

In addition to the prohibition of bulk collection in the US under section 702, (targeting) requests have to be documented, and national intelligence priorities are established on the basis of publicly available process. In case of incidents or improper tasking, the US representatives indicated that the data is purged in most cases. For National Security letters, queries also have to rely on a reasonable belief that the data are necessary.

The European authorities asked for **quantitative and/or qualitative elements to validate the amount of data collected under the different authorities**, also in order to show that since the adoption of the Privacy Shield the collection of personal data is "as tailored as feasible" (as said in the Presidential Policy Directive 28, or PPD-28) and that **access to data is restricted to what is necessary**. The US authorities indicated that some elements are set out in the transparency report of the Privacy and Civil Liberties Oversight Board (PCLOB) on section 702, and that they could not give much more information, especially to explain the numbers (either why the number of targets under section 702 increase while the number of National Security letters diminishes, or the number of connections corresponding to the number of targets), as more information could result in the information of the targets concerning their surveillance.

6.2.4 Executive Order 12333

On Executive Order (EO) 12333, questioned on this subject, the US representatives underlined that requests under this instrument are not alternatives to requests addressed to the companies within the US territory. However, they confirmed that this EO allows for the interception of data undergoing transfer to the US and that PPD28 also applies in this context, without providing numbers on the amount of data collected or interpretations of the relevant parts of PPD-28 beyond the assurances and examples provided in the letter of General Counsel of the ODNI of last year.

6.2.5 PPD28

The representatives of US authorities confirmed that the new Administration continues to be committed to PPD-28, and that it has been translated into all minimization procedures of the agencies. Further questioned on EO 12333, they indicated that targeting is necessary in order to avoid being overflowed with information, for instance to limit to a certain area of the world, while using both location and technology to target the collection. They also referred to a report on bulk collection by the National Academies Press.

The authorities also indicated that two standards have been issued on PPD28: EO 13462 on the obligation to report violations of PPD28 and a standard on the retention of data.

Questioned on the role of Privacy Officers, they indicated that they work with the agencies, including with the technicians, in order to ensure that the rules are respected, and that all the necessary information are transmitted to the PCLOB. In case of compliance incidents, they indicated they looked at: system problems, issues with individual employees or if training is needed, data improperly collected our used. They also underlined the role of NSA Inspector General.

6.3 Redress:

The presentation started with elements on **Freedom of Information Act[38] (FOIA)**, which does not provide redress but provide for the right to access documents. FOIA provides a general right of access to documents as well as the right for individuals to request their own data under the statute. Anyone can submit a request under FOIA and there are court deadlines.

It was followed by a presentation of the **Administrative Procedure Act[39] (APA),** a general statue for people who have suffered maladministration from public authorities, when there are no other remedies foreseen in a specific text.

Questioned on the possible protection that APA could offer to European as regards FISA, the US representative indicated that redress and remedies are already foreseen in FISA, so that APA may be of less relevance. In addition, the standing requirement needs to be met in the context of FISA and APA claims.

Further questioned on the possibility to use APA to act against minimization procedures or claim that there has been a violation of PPD28, and more generally on what can be referred upon under this Act, no answer was provided, except that PPD28 has to be translated into the statutes of the IC. Therefore, actions could only be brought against the statutes.

On the **effective remedies available**, and especially confronted with the claim of ACLU that, to date, no civil lawsuit challenging section 702 or EO 12333 surveillance has ever produced a US court decision addressing the lawfulness of surveillance measures, they indicated that service providers can oppose the order and that it had already been done, and underlined that in criminal proceedings, some court cases challenged the legality of section 702.

[38] 5 U.S.C. § 552
[39] 5 U.S.C. § 702

They also indicated that a **civil case is currently ongoing**. The **question of standings is under examination**.

They stressed that since two years, the possibility to challenge 702 orders was introduced under the USA Freedom Act (National Security Letters recipients can now challenge non-disclosure orders).

*
* *

7. Oversight by the Inspector General

The General Counsel for the Inspector General (IG) of the Intelligence Community (Ms Jeannette McMillian) presented her work and answered questions.

She reminded the participants that **IGs are appointed and removed by the President**, and **confirmed by the Congress**.

She recalled that IGs' tasks are to **audit the tools**, **detect frauds and misconducts** and more generally **verify that data are processed in compliance with the applicable rules**. Therefore they have **independent access to information**, and recent legislation has boosted IGs functions.

They can work with whistleblowers, and also have independent budget ("yet very limited"). They can also support civil liberties officers.

IGs also **present reports every six months** which are to the directors, as well as to the Congress, which include findings (on whether there have been violations or not), **as well as recommendations to resolve the problems** when there are. Both would be presented to the Ombudsperson.

Questioned on the **content of the report in cases where no violation was found**, she underlined that in any case IGs could recommend improvements and report these recommendations to the Congress.
She underlined the effort towards transparency, and the possibility to have classified elements annexed to the reports.

Questioned on the **scope of the compliance review performed**, she recognized that IGs can only verify the compliance with the applicable rules (and not the rules themselves).

Eventually, questioned on the **limits foreseen to the dismissal of IGs**, she indicated that although no limit are expressly foreseen, a 30-day delay runs between the decision and the dismissal, allowing therefore to ask the reasons for the dismissal. To her recollection, IGs have only been dismissed for personal misconduct.

*
* *

8. Ombudsperson Mechanism.

8.1 Ombudsperson's team

The **Acting Ombudsperson** presented her team (Mr Robert Strayer, the head of the Ombudsperson's secretariat was appointed three days before this meeting and was present).

She indicated that there is **still no date for the nomination of a formal Ombudsperson**, but that in the meantime she is fully committed and empowered to execute her missions and underlined that she is independent from the IC community and free from improper influence.

8.2 Independence

To a question on the independence of the Ombudsperson, the US authorities replied that even in the absence of a binding inner procedure to deal with idependence problems, should a concern in relation to the independence of the Ombudsperson arise, the undersecretary of State could (this is optional) go directly to the Secretary of State. However, the nomination and revocation process do not include a warning period. Ultimately, the power to nominate or revoke the Ombudsperson belongs to the Secretary of State.

8.3 Procedures of the Ombudsperson

The team of the Ombudsperson also presented the **implementation of the procedures of the Ombudsperson** (the **unclassified procedures only**), and presented **the website** of the Ombudsperson. They underlined that the Ombudsperson's process is very robust. They also indicated that so far they have:

- Set up internal procedures,
- Stood up the website,
- Put in place inter-agency agreements,
- Done a PIA for the records system, available on the Department website,
- Recorded a notice,
- Recorded disposition schedule.

Concerning the implementation procedures, they indicated that they aim at assigning responsibilities. They also stressed that only 2 individuals in the State Department have access to the website, and confirmed that, while a **"unique identifier"** is a requirement to consider the request complete, the identifier is not limited to an email address.

Questioned on the **classified part of the procedures**, they indicated that they concerned the handling of compliance incidents and how to process the information, and that they would not grant access to any further document or information concerning them. They also stressed the multilayered approach to compliance and underlined that there was no general process to deal with the cases and that they intended to process the requests on a case by case basis and thus that mechanisms could change accordingly ("we need to provide space to adapt to the reality"). No further questions were permitted as to the cooperation of the Ombudsperson with the intelligence community in response to a request submitted to the Ombudsperson.

Questioned on their role in the context of the Ombudsperson, the Inspector General underlined that IGs can receive referrals from other authorities, for instance from Congress, and check if an audit is necessary, while proceeding to a systematic review.

Further questioned on how an IG would interact with the Ombudsperson, she indicated that the Law foresees that IGs' access to data in the field of National Security can be limited by the Director of the Agency. In case of such limitations, the Director of the agency has to inform the Congress of the denial of access, as well as of the reasons why. Eventually, the IG comes back to the person or the referring authority with as many declassified information as possible.

8.4 Processing of requests by the Ombudsperson

On the **processing of requests by the Ombudsperson**, they underlined that if a request seeks information linked to an email address only, this request may be treated under FOIA. In response to a question, it was confirmed however that a request under the Ombudsperson mechanism would also generally be interpreted to fall under the Ombudsperson mechanism rather than FOIA.

They also confirmed that there could be exceptional sharing of information with other authorities on an individual basis and that senior authorization would be needed.

8.5 Retention periods

On the retention periods, they indicated that they are still in the process of setting them, but aimed at ensuring that the data will only be held for the minimum amount of time necessary, and that this would not be for more than 5 years, as it is the current period for which FOIA request are stored.

8.6 Remedies

They also indicated that among the appropriate remedies they could propose training of individuals and purging of data.

At the end of this session, they indicated they could send examples of how they would deal with specific cases in order to provide illustrations of their procedures. The unclassified Implementation Procedures of the Ombudsperson, presenting additional information as regards the independence of the Ombudsperson and examples illustrating how cases would be handled in coordination with the other competent authorities, were shared later. The applicable procedures remain classified.

*

* *

9. PCLOB

The **only left PCLOB member**, Ms Elisebeth Collins, presented the work of the PCLOB.

She underlined that with her **individual Board capacity**, she can do a Board member statement, and that she can continue performing her advisory function, as well as the projects still ongoing (e.g.

report on EO 12333). However she cannot do a Board Report and no new project can be started. She underlined that a Chair was nominated the 5 September, although he has not been confirmed by Congress yet. 20 persons in the staff are still working.

She confirmed that the **report on PPD-28 was voted in December 2016**, and passed to the President, but that parts remain classified and subject to **Presidential privilege**.

Questioned on the **report on EO 12333**, she confirmed that work is still ongoing, but that they would need a quorum of the Board to vote on whether to issue it or not.

She also indicated that she could lead interviews although she might not be in a formal position to conduct hearings.

*

* *

10. EU Presentation and Program implementation

A session was organized to allow the European participants to explain how they have implemented their own obligations under the Privacy Shield and to present their actions to "advertize" on the Privacy Shield.

The Commission presented its actions towards stakeholders (citizens guide), animations for awareness-raising and meetings organized.

The Review team presented the actions undertaken, especially the publication of the referral forms, the setting up of an EU centralized body and underlined that no cases have been brought to date.

The DoC asked several questions to the Commission and the Review team on the actions undertaken on the EU side (publication of the internal policies of the EU DPAs, of the questionnaires, on the questions and inquiries, from individuals as well as from companies, received by the EU DPAs).

The DoC also asked how they could jointly communicate with EU DPAs to address the lack of confidence in the Privacy Shield.