EUROPEAN
COMMISSION

Brussels, 23.10.2019
SWD(2019) 390 final

COMMISSION STAFF WORKING DOCUMENT
Accompanying the document

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the third annual review of the functioning of the EU-U.S. Privacy Shield

{COM(2019) 495 final}

1. INTRODUCTION

This document presents the findings of the Commission services on the implementation and enforcement of the EU-U.S. Privacy Shield framework (the "Privacy Shield") in its third year of operation. The findings are based on information gathered from relevant stakeholders and U.S. authorities both in the preparation of and during the Annual Joint Review meetings held in Washington, D.C. on 12 and 13 September 2019. As in previous years, the findings have been further informed by publicly available material, such as court decisions, implementing rules and procedures of relevant U.S. authorities, reports and studies from non-governmental organisations, transparency reports issued by Privacy Shield-certified companies, annual reports from independent recourse mechanisms, as well as media reports. The eight representatives designated by the European Data Protection Board [1] (the "EDPB") to participate in the Annual Joint Review together with the Commission, have been consulted on this document and provided feedback on the factual findings.

This document follows the same structure as the Commission Staff Working Documents from the first and second annual review in 2017 and 2018.[2] It provides an update on developments concerning the functioning of the framework which took place since last year's annual review and looks at elements that newly emerged in the context of the third annual review. For detailed explanations on the relevant Privacy Shield requirements and obligations for each of the aspects covered, as well as on developments that took place before the second annual review, the Commission services refer to the Staff Working Documents on the first and second annual review. For ease of reference, this document follows the same structure as the previous Staff Working Documents.

2. THE FIRST AND SECOND ANNUAL REVIEW – OUTCOME AND RECOMMENDATIONS

On 12 July 2016, the Commission adopted a Decision[3] (the "adequacy decision") in which it found that the EU-U.S. Privacy Shield ensures an adequate level of protection for personal data that has been transferred from the EU to organisations in the U.S. The adequacy decision provides for an annual evaluation of all aspects of the functioning of the framework by the Commission.[4]

[1] The European Data Protection Board is an independent body composed of representatives of the national data protection authorities of the EU Member States and the European Data Protection Supervisor.

[2] Commission Staff Working Document Accompanying the 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 (SWD(2017)344 final), see http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619, and Commission Staff Working Document Accompanying the Report from the Commission to the European Parliament and the Council on the second annual review of the functioning of the EU-U.S. Privacy Shield (SWD(2018) 497 final), see https://ec.europa.eu/info/sites/info/files/staff_working_document_-_second_annual_review.pdf.

[3] 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 2017, 1.8.2016, p. 1.

[4] Recitals 145-149 of the adequacy decision.

The first Annual Joint Review took place on 18 and 19 September 2017 in Washington, D.C. On 18 October 2017, the Commission adopted its report to the European Parliament and the Council,[5] accompanied by a Commission Staff Working Document.[6] In its report, the Commission noted that the U.S. authorities had put in place the necessary structures and procedures to ensure the correct functioning of the Privacy Shield. On the basis of its findings from the first review, the Commission concluded that the U.S. continued to ensure an adequate level of protection for personal data transferred under the Privacy Shield from the Union to organisations in the United States. At the same time, the Commission considered that the practical implementation of the Privacy Shield framework could be further improved in order to ensure that the guarantees and safeguards provided therein continued to function as intended. To this end, the Commission made ten recommendations.[7]

The second Annual Joint Review took place on 18 and 19 October 2018 in Brussels. The Commission adopted its report to the European Parliament and the Council,[8] accompanied by a Commission Staff Working Document,[9] on 19 December 2018. On the basis of its findings from the second annual review, the Commission confirmed that the U.S. continued to ensure an adequate level of protection for personal data transferred under the Privacy Shield. In particular, the Commission noted that the steps taken to implement the Commission's recommendations from the first annual review had improved several aspects of the practical functioning of the framework, such as the introduction by the the Department of Commerce (the "DoC") of new mechanisms to detect potential compliance issues, more proactive monitoring of compliance by the Federal Trade Commission (the "FTC"), public release by the Privacy and Civil Liberties and Oversight Board (the "PCLOB") of its report on the implementation of Presidential Policy Directive 28, etc. However, as some of these steps had been taken just before the second annual review and certain processes were still ongoing, the Commission concluded that further developments concerning these processes and mechanisms required close monitoring. Moreover, while the function of the Ombudsperson under the Privacy Shield was carried out by an Acting Under Secretary of State and the Ombudsperson mechanism was thus fully functioning, the Commission had stressed the importance of filling the position of the Privacy Shield Ombudsperson on a permanent basis and, in particular, called on the US government to identify a nominee for this position before 28 February 2018.[10] The elements identified in the second annual review as requiring close monitoring are referrred to in the relevant sections of the present document.

[5] 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, see http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619.
[6] See footnote 2.
[7] See Commission Report on the first annual review, p. 4-7.
[8] Report from the Commission to the European Parliament and the Council on the second annual review of the functioning of the EU-U.S. Privacy Shield (COM(2018) 860 final, see https://ec.europa.eu/info/sites/info/files/report_on_the_second_annual_review_of_the_eu-us_privacy_shield_2018.pdf
[9] See footnote 2.
[10] See Commission Report on the second annual review, p. 4-6.

3. THE THIRD ANNUAL REVIEW – PREPARATION AND CONSULATION OF STAKEHOLDERS

In its third year of operation, the Privacy Shield has moved from the inception phase to a more operational phase. All components of the Privacy Shield framework as agreed between the EU and the U.S. are in place. Privacy Shield-certified companies are applying the Privacy Shield Principles in their day-to-day business and the relevant U.S. authorities have made use of the various tools, mechanisms and procedures developed for administrating, overseeing and enforcing the Privacy Shield framework. The third annual review therefore focused on the effectiveness of these tools, mechanisms and procedures in practice, notably with respect to those that were identified in the second annual review as requiring further monitoring.

On 18 June 2019, the Commission services sent questionnaires to ten trade associations in the U.S.[11] to collect input from those of their members that are Privacy Shield-certified. The questionnaires focused on the practical experience of Privacy Shield-certified companies and covered a wide range of issues relating inter alia to the (re)certification process, steps taken to comply with the Privacy Shield Principles, including with the Accountability for Onward Transfers Principle, internal mechanisms to deal with requests and complaints from data subjects, as well as the processing of human resources data, automated decision-making and requests for access to data by public authorities.

On the same day, the Commission services also sent questionnaires to eight Non-Governmental Organisations (NGOs) which are active in the field of fundamental rights and in particular digital rights and privacy.[12] The questionnaire sought input on relevant developments in the U.S. legal framework, oversight and enforcement mechanisms, the functioning of redress and review mechanisms and automated decision-making.

The Commission received written replies to its questionnaires from trade associations and NGOs in July 2019. Throughout the entire preparatory phase, the Commission services had exchanges with trade associations, individual companies and NGOs to follow-up on the input provided. This notably included meetings with industry and business associations on 9 September 2019 and with NGOs on 11 September 2019.

In order to prepare the discussion at the annual review meetings, the Commission services also sent a detailed set of questions to the U.S. authorities that administer, oversee and enforce the Privacy Shield framework. In the course of 2019, the U.S. authorities had informed the Commission services of certain developments relevant to the Privacy Shield, notably about appointments to key oversight bodies and relevant enforcement actions taken by the FTC.

[11] Namely, Software& Information Industry Association, U.S. Chamber of Commerce, Information Technology Industry Council, The Software Alliance, Centre for Information Policy Leadership, Internet Association, Interactive Advertising Bureau, United States Council for International Business, Computer & Communications Industry Association and Engine.

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

Following the designation by the EDPB of its representatives to the annual review during the Plenary meeting in May 2019, the Commission services met them (on 3 and 11 September 2019) to prepare for the Annual Joint Review, discuss the input received and identify which aspects require additional information-gathering and clarification.

The Commission also kept the EU Member States closely informed and received their feedback, notably in a meeting of the Council Working Party on Information Exchange and Data Protection ("DAPIX") on 3 September 2019. In parallel, the Commission had exchanges with the European Parliament on the preparation of the third annual review, in particular in the context of a meeting of Commissioner Jourová with the LIBE Committee on 22 July 2019.

4. THE THIRD ANNUAL REVIEW – PROCESS AND FINDINGS

The third Annual Joint Review took place in Washington, D.C. on 12 and 13 September 2019. On the U.S. side, representatives from the Department of Commerce, the Department of State, the Federal Trade Commission, the Department of Transportation (the "DoT"), the Office of the Director of National Intelligence (the "ODNI"), the Department of Justice (the "DoJ") and the Privacy and Civil Liberties Oversight Board participated in the review, as well as the Inspector General for the Intelligence Community and the newly appointed Ombudsperson .

In addition, representatives from two organisations that offer independent dispute resolution services under the Privacy Shield and the American Arbitration Association that administers the Privacy Shield arbitration panel provided information during the relevant review sessions. Finally, the review was informed by presentations by two Privacy Shield-certified organisations[13] on how companies comply with the requirements of the framework.

The review was opened by Director-General for Justice and Consumers Tiina Astola, U.S. Secretary of Commerce Wilbur Ross, FTC Chairman Joseph Simons and Vice Chair of the EDPB Ventsislav Karadjov. It was conducted for the EU by representatives of the European Commission's Directorate General for Justice and Consumers. The EU delegation also included eight representatives designated by the EDPB.

The review meeting was organised by topic, with each dedicated agenda point introduced by a short presentation by the relevant U.S. authority or organisation, followed by a detailed question-and-answer session. It covered the "commercial aspects" of the framework (i.e. aspects relating to certified companies' compliance with the Privacy Shield's requirements as well as to the administration, oversight and enforcement of such requirements by the competent US authorities) on the first day and issues concerning government access to personal data on the second day.

4.1. COMMERCIAL ASPECTS

[13] Workday and Relx.

With respect to the commercial aspects, the Commission assessed the concrete functioning of the administration, oversight and enforcement of the Privacy Shield process. In light of the findings of last year's annual review, the third annual review focused notably on the re-certification process, compliance monitoring and enforcement. As in previous years, the review also looked at developments concerning two substantive topics: human resources data and automated individual decision-making. Finally, the review took into account developments in U.S. law which have taken place since the second annual review and could be relevant for the functioning of the commercial aspects of the Privacy Shield.

4.1.1. The (re)-certification process

At the time of the review meetings, just over 5,000 companies were certified under the Privacy Shield. After three years of operation, the Privacy Shield has therefore more participating companies than its predecessor, the Safe Harbor arrangement, had obtained after 13 years of existence (i.e. just over 4,000 participants), including a number of U.S. subsidiaries of EU headquartered companies.[14] The majority (more than 70%) of Privacy Shield certified-companies are Small and Medium-sized entreprises (SMEs). The success of the Privacy Shield is also reflected in the current re-certification rate of 89%.[15]

With respect to first-time certifications, the DoC informed that since the second annual review it had rejected nine applications for certification. In five of these cases, the applicants were companies not established in the U.S., which are not eligible to participate in the framework. In the remaining cases, the companies did not qualify to participate in the framework because they were non-profit organizations and were not subject to the jurisdiction of the FTC or the DoT.[16] As also confirmed by the responses from trade associations to the Commission's questionnaire, the completion of the first-time certification often requires a significant back-and-forth between the company applying for certification and the DoC, as the DoC identifies shortcomings in the company's application which it asks the company to rectify, thereby triggering a process of consultation between the DoC and the company concerned.[17]

The DoC also confirmed that it continues to apply the changes that were made to the certification process further to the Commission's recommendations after the first annual review. The DoC now requests first-time applicants not to make any public representations about their participation in the Privacy Shield before the DoC has finalised their certification. To this end, applicants are required to submit their draft privacy policies for review, which

[14] Studies suggest that around 200 U.S. subsidiaries of EU companies are certified under the Privacy Shield, see https://fpf.org/2019/09/09/new-fpf-study-more-than-200-european-companies-are-participating-in-key-eu-us-data-transfer-mechanism/.

[15] The Privacy Shield is not only important for Privacy Shield-certified companies in the U.S., but also for EU companies that rely on it in order to transfer personal data to their subsidiaries and business partners in the U.S. without any additional requirements or costs.

[16] For further explanations, see Letter from Federal Trade Commission Chairwoman Edith Ramirez, Annex IV of the adequacy decision, and Letter from U.S. Secretary of Transportation Anthony Foxx, Annex V of the adequacy decision.

[17] See section 4.1.1 of the Commission Staff Working Document on the first annual review, p.6.

are made public only after the DoC has confirmed that the applicant fulfills all certification requirements. Once the privacy policy is public, the company notifies the DoC, which then includes the company on the Privacy Shield list without delay.[18] The Commission services stress the importance of this change in procedure for avoiding legal uncertainty and false claims of participation in the framework.

However, it emerged at the third annual review that the procedure followed by the DoC in the context of re-certification raises issues that are in part similar to the ones described above. For an extended period of time, companies that have not submitted their re-certification application before their certification has lapsed or that are still in the process of re-certification after their certification has lapsed, continue to be listed as "active" Privacy Shield participants and to publicly refer to their adherence to the Privacy Shield, although they may eventually never complete the re-certification process.

The DoC explained that while companies are expected to submit their annual re-certification application before the re-certification due date, there is a "grace period" of 30 days in which the DoC still accepts a company's re-certification application. Once a company has submitted its re-certification application (which may be at the very end of the "grace period"), it has 45 days to complete the process. If the DoC detects in its quartely review for false claims of participation in the framework (see below, Section 4.1.2) that the company did not complete the process, the DoC sends a warning letter, which gives the company another 30 days to finalise the re-certification. Only if the company does not do so within this timeline it is removed from the Privacy Shield list and moved to the "inactive" list. As a consequence, a company may remain on the Privacy Shield "active" list for a total period of 105 days (approximately 3.5 months) beyond the re-certification due date, or, depending on when the DoC detects that the company did not complete the process, for even a longer period of time.

Similarly, and as already discussed during the second annual review, the re-certification process is sometimes initiated before the re-certification due date, but still continues after this date has lapsed, for example because of confusion about formal requirements, such as the payment of fees, which require a back and forth between the DoC and the company. While the DoC at the last annual review had provided reassurance that the re-certification would have to be finalised within 45 days after the due date,[19] the company in fact receives a further "grace period" of 30 days to complete the re-certification process. Moreover, it may take some time until the DoC detects in the context of its quarterly review for false claims that the re-certification was not finalised.

The Commission services fully understand the DoC's intention to support companies in obtaining re-certification, as it is preferable for the protection of individual's privacy to have more companies adhering to the framework and complying with its requirements. The Commission services are also aware that the obligations under the Privacy Shield remain fully enforceable for as long as a company is listed as participating in the Privacy Shield, and

[18] See section 4.1.1 of the Commission Staff Working Document on the second annual review, p.6.
[19] See section 4.1.1 of the Commission Staff Working Document on the second annual review, p.7.

violations of the Privacy Shield Principles that occur before the re-certification process is completed can therefore be investigated and followed-up upon by the FTC. Nevertheless, the Commission services consider that the period during which companies may remain on the Privacy Shield "active" list without having completed the re-certification process is too long. A period of more than three months in which a company's re-certification due date has lapsed while the company continues to be listed as active Privacy Shield participant does not only reduce the transparency and readability of the Privacy Shield list for both businesses and individuals in the EU, but also does not incentivise participating companies to rigourously comply with the annual re-certification requirement.

The Commission services take the view that this issue is not resolved by the change of procedure that was introduced by the DoC in August this year. According to the new procedure, the next re-certification due date that is indicated on the Privacy Shield list is no longer 12 months from the date at which the previous re-certification was completed, but from the date at which the company submitted the application for re-certification. While this change in procedure reduces the incentive for companies to (unnecessarily) prolong the process for completion of the re-certification (as the next re-certification due date is based on the date of submission) and is therefore a welcome improvement of the process, it does not address the issue of the transparency of the Privacy Shield "active" list. A company may still be listed as active Privacy Shield participant although the re-certification due date lies several months in the past. As mentioned above, this creates uncertainty and should be addressed by shortening the time/"grace" periods that are granted to companies in the various steps of the re-certification process.

At the third annual review meeting the DoC also informed that it has undertaken further steps to improve and accelerate the re-certification process. Since August 2019, the DoC sends the automatic e-mail reminders which are sent out one month, two weeks and one day before the next re-certification due date to all points of contact that have been designated by a company. In the past the DoC had encountered difficulties where, due to staff turnover in companies, single points of contact had changed or were no longer available and automatic reminders and updates were therefore not received. The DoC had thus asked companies to provide multiple points of contact.[20]

At the date of the third annual review meeting, around 450 companies were on the "inactive" list on the Privacy Shield website. These are the companies that failed to submit their annual re-certification in a timely manner, failed to complete the re-certification process in a timely manner or withdrew voluntarily. According to the DoC, in the Privacy Shield's third year of operation approximately 230 companies were removed from the "active list" because they either failed to successfully complete the annual recertification, failed to successfully complete the annual recertification process, failed to address certification compliance issues raised by the DoC, or failed to respond to requests from the DoC, while 39 companies voluntarily withdrew from the Privacy Shield.

[20] See section 4.1.1 of the Commission Staff Working Document on the second annual review, p. 7.

The Commission services positively noted that the dialogue between the DPAs and the DoC in the context of the annual review has led to a review of the certification status of a number of companies on the Privacy Shield list by the DoC, in the course of which shortcomings were identified and remedied.[21]

The Commission services welcome that the DoC continously reviews the (re-)certification process and amends it to address issues as they arise. At the same time, the Commission services stress the importance of the transparency and readability of the Privacy Shield "active" list and urge the DoC to shorten the time periods that are granted to companies for completing the re-certification process. For instance, a period of maximum 30 days in total would seem reasonable to allow companies sufficient time for re-certification, including forrectifying any issue identified in the re-certification process, while at the same time ensuring the effectiveness of this process. If at the end of this period the re-certification is not completed, the DoC should send out the warning letter without further delay.

4.1.2. Monitoring and supervision by the Department of Commerce

In its report on the second annual review, the Commission had concluded that it would closely monitor the effectiveness of the mechanisms introduced by the DoC in the second year of operation of the Privacy Shield to proactively monitor compliance by certified companies with the Privacy Shield Principles, in particular compliance with substantive requirements and obligations.[22]

One of these mechanisms are the so-called "spot-checks", by which the DoC randomly selects companies to verify whether 1) point(s) of contact for handling complaints, access requests, and other issues arising under the Privacy Shield are available and responsive; 2) the organisation's privacy policy is freely and openly available; 3) the organisation's privacy policy continues to comply with the certification requirements and 4) the organisation's chosen independent resolution mechanism is available to handle complaints. If the DoC finds that there is credible evidence that a company does not comply with its commitments, it sends a Compliance Questionnaire to which the company must respond within 30 days.[23] If there is no timely and satisfactory response, the DoC sends a certified warning letter requiring the company to indicate within 30 days how it has addressed the detected issue(s). If the issue(s)

[21] A search of the Privacy Shield "active" list that was carried out by the Data Protection Authority of Hessen (Germany) in August 2019 revealed that approximately 300 companies were listed as "active", while their re-certification due date was in the past. In about 30 cases, the re-certification due date dated back to 2018. In the context of the third annual review, the results of this search were transmitted to the DoC, which investigated all the listed cases and took follow-up action where necessary. In 110 cases, the companies had finalised the re-certification process in the meantime. In 119 cases, the DoC removed the company from the Privacy Shield "active list". In 73 cases, the re-certification process was still ongoing at the time of the adoption of this document.

[22] See Commission Report on the second annual review, p. 5.

[23] The DoC's Questionnaire is standardised but requires companies to indicate specific information regarding occurred incidents and compliance concerns.

would not be resolved by the end of that 30-day period, the organisation would be removed from the Privacy Shield list, placed on the "inactive" list and referred to the FTC.[24]

At this year's annual review, the DoC explained that it has continued to carry out the above-mentioned spot-checks. These are now being carried out in a more regular and systematic manner, as the DoC introduced in April 2019 a system in which it checks 30 companies each month. In about 28% of the spot-checks carried out, the DoC detected potential compliance issues and sent out the Compliance Questionnaire. The most common issues of non-compliance that were detetected concerned the lack of response from designated points of contact and the inaccessibility of a company's privacy policy online. In most of the detected cases, the DoC did not have to send out warning letters, as the companies responded to the Questionnaire and rectified the detected issues. Since the last annual review, warning letters have been sent out in only three cases, and no compliance issues detected under the spot-check procedure have been referred to the FTC.

The Commission services welcome that the DoC is carrying out proactive compliance spot-checks on a regular basis and in a systematic manner, which is important for improving the overall compliance with the framework and for detecting cases that may require enforcement action by the FTC. However, the spot-check process should not be limited to formal requirements, such as the responsiveness of contact persons and the availability of privacy policies. Instead, the DoC should also check more substantive requirements, for example assessing compliance with the Accountability for Onward Transfers Principle by requesting a summary or a representative copy of the privacy provisions of a contract concluded by a Privacy Shield-certified company to transfer personal data to a third party acting as agent (i.e. a possibility expressly provided for by the Privacy Shield framework).[25] The requirements for onward transfers have been significantly strengthened in the Privacy Shield, as a lack of safeguards in such situations would undermine the protections guaranteed by the framework. Whereas the spot-checks should continue to be done regularly and in a systematic manner, compliance with these requirements is thus crucial for the continuity of the Privacy Shield and should be subject to strict monitoring and enforcement by the U.S. authorities.

Aside from the spot-checks, the DoC had also developed additional compliance review procedures. Notably it had reported that one member of the DoC Privacy Shield team is responsible for the monitoring of public reports (e.g. media articles) about the privacy practices of Privacy Shield participants. If the DoC finds that there is credible evidence that compliance with the Privacy Shield Principles could be affected, it initiates the compliance process by sending the Compliance Questionnaire.[26]

With respect to the oversight role of the DoC regarding false claims of participation in the Privacy Shield framework, the Commission concluded in its report on the second annual

[24] See section 4.1.2 of the Commission Staff Working Document on the second annual review, p.8-11.
[25] See Annex II Section II Principle 3(b) of the adequacy decision.
[26] See section 4.1.2 of the Commission Staff Working Document on the second annual review, p.9. During the third annual review meeting, the DoC informed that it had made use of this mechanism three times, including vis-à-vis Facebook further to the FTC settlement of 23 July 2019 (see below, Section 4.1.3.).

review that it would closely monitor the effectiveness of the tools introduced by the DoC to detect false claims, with a particular focus on the search of false claims by companies that have never applied for certification.

At the third annual review, the Commission services noted that the DoC had continued to search for false claims of participation on a quarterly basis, targeting organisations that 1) started but did not complete their initial certification, 2) started but did not complete their re-certification and 3) did not submit their annual re-certification. Through this process, the DoC detected 669 cases of false claims of particpation since the last review in October 2018. In all these cases, the DoC sent certified warning letters to the companies concerned. In most cases, companies completed their (re-)certification further to these warning letters. In some instances, companies decided to withdraw from the Privacy Shield. Companies that did not complete the re-certification and did not remove public references to their participation in the Privacy Shield within the indicated timeframe of 30 days were referred to the FTC. Since the last review, the DoC referred 143 cases of false claims of participation to the FTC. In most cases, the referral itself was sufficient to ensure that the concerned company took the necessary action to resolve the identified issue.

The DoC also informed that a general search for false claims of participation on the internet had proven to be of limited utility. At the time of the third annual review, the DoC had therefore not yet conducted a systematic search for false claims by companies that have never been part of the framework. Instead, it was still in the process of looking for technical solutions such as "web crawls" to detect this kind of false claims. Pending such a technical solution, the DoC relies on referrals from the public or other sources to identify false claims from companies that have never applied for certification.

The Commission services regret that the DoC does currently not have appropriate tools at its disposal to more effectively identify false claims of participation in the framework by companies that have never applied for certification. The rather high number of false claims of participation detected by the DoC (which in many cases required also a referral to the FTC) confirms that false claims represent a real issue. Fromall kinds of false claims, those false claims from companies that never applied for certification are the potentially most harmful. This is true from the point of view of individuals' privacy, as companies that have never applied for certification have not implemented any of the protections guaranteed by the Privacy Shield in their business practices. It is also true from a business' perspective, since the level playing field between companies is weakened if organisations, which are not complying with the requirements of the framework, can claim the benefits of certification, which then negatively impacts the overall credibility of the framework. The DoC should therefore make it a priority to develop tools for detecting this kind of false claims, and use these tools in a regular and systematic manner.

4.1.3. Enforcement by the Federal Trade Commission

In its report on the second annual review, the Commission concluded that it would monitor the progress and outcome of the *ex officio* "sweeps" carried out by the Federal Trade

Commission (FTC) in the second year of operation of the Privacy Shield by means of administrative subpoenas to detect substantive violations of the Privacy Shield.[27]

In this respect, during the the third annual review the FTC informed that, since last year, including as a result of the announced *ex officio* sweeps, it concluded seven enforcement actions related to Privacy Shield violations.[28] All seven cases concerned false claims of participation in the framework by companies that either failed to complete the necessary steps to obtain certification from the DoC (LotaData, Inc., DCR Workforce, Inc., Thru, Inc., Trueface.ai.[29] and Secur Test Inc.[30]) or allowed their certification to lapse, but misrepresented their continued participation in the program (EmpiriStat, Inc.[31] and Cambridge Analytica[32]). Both for EmpirStat and Cambridge Analytica, the FTC also alleged a violation of Supplemental Principle 6 of the Privacy Shield, as they failed to affirm to the DoC that, after they stopped their participation in the framework, they continued to apply the Privacy Shield protections to personal information collected while participating in the program. Moreover, with respect to EmpirStat, the FTC alleged a violation of Supplemental Principle 7 of the Privacy Shield for a failure to verify, through a self-assessment or by means of an outside compliance review, that the assertions the company makes about its Privacy Shield practices are true and that those practices have been implemented. All actions were concluded with a settlement with the respective company that committed for the future not to misrepresent its participation in the framework and its adherence to the Privacy Shield Principles.

The Commission services welcome the enforcement action taken by the FTC in the third year of operation of the Privacy Shield. At the same time, in light of the agency's announcement of last year and the assurances provided in the course of the second annual review,[33] the Commission services would have expected a more vigourous approach regarding enforcement action on substantive violations of the Privacy Shield Principles. In this respect, the Commission services take note of the information provided at the third annual review meeting that a number of ongoing investigations are taking more time, as the FTC is looking at the full range of possible violations.

Nevertheless, and while taking into account relevant confidentiality considerations, it does not appear justifiable that the FTC cannot share, even in an aggregate and/or anonymous form, information on the *ex officio* sweeps that are being carried out. This approach is not

[27] Commission Report on the second annual review, section 2, p. 5. See also section 4.1.3 of the Commission Staff Working Document on the second annual review, p. 17.

[28] See also the remarks by FTC Chairman Simons: https://www.ftc.gov/system/files/documents/public_statements/1543886/simons_-_privacy_shield_remarks_9-12-19_0.pdf

[29] See FTC Press release https://www.ftc.gov/news-events/press-releases/2019/09/five-companies-settle-ftc-allegations-they-falsely-claimed

[30] See FTC Press release https://www.ftc.gov/news-events/press-releases/2019/06/ftc-takes-action-against-companies-falsely-claiming-compliance-eu

[31] See FTC complaint and the agreed consent order https://www.ftc.gov/enforcement/cases-proceedings/182-3195/empiristat-matter

[32] See FTC Press release https://www.ftc.gov/news-events/press-releases/2019/07/ftc-sues-cambridge-analytica-settles-former-ceo-app-developer

[33] See Section 4.1.3 of the Commission Staff Working Document on the second annual review, page 17.

only not in line with the spirit of cooperation among authorities on which the framework is based, but also does not allow the Commission to be appropriately informed about relevant developments for its annual evaluation of the functioning of the framework.[34] The Commission services therefore consider that the FTC should, as a matter of priority, find ways to share meaningful information on ongoing investigations with the Commission as well as with EU DPAs that also have enforcement reponsabilities under the Privacy Shield (either because the transfer in question involves HR data or because the company in question has opted for the EU DPA Panel to act as its independent recourse mechanism). To the extent it would be necessary to further develop the cooperation between the Privacy Shield's co-enforcers, more formal solutions should be explored, building for example on the enforcement cooperation agreement being negotiated in the area of consumer protection.

More generally, the Commission services note that it has been an important year for the FTC's enforcement actions in the area of privacy. In particular, two major settlements were reached for alleged violations of the Children's Online Privacy Protection Rule ("COPPA"). The first case resolved the charges against YouTube to have illegally collected personal information from children—including in the form of persistent identifiers—without their parents' consent. As a result of this settlement, YouTube (and its parent company Google) agreed on a $170 million penalty.[35] The second case, settled with a penalty of $5.7 million, concerned the FTC's allegations against the Video Social Networking App Musical.ly (known as TikTok) for having illegally collected personal information from children without parental consent.[36] In addition, in the context of a data breach investigation against Equifax, the FTC concluded a settlement with the company to pay at least $575 million, and potentially up to $700 million.[37]

Finally, the agency concluded a settlement with Facebook alleging the violations of a 2012 FTC order and the FTC Act, by engaging in practices deceiving users about their ability to control the privacy of their personal information.[38] As part of the settlement, the company will pay a penalty of $5 billion and will submit to new restrictions and a modified corporate structure.

During the third annual review meeting, the FTC provided a number of clarifications on the Facebook settlement and its relation to the Privacy Shield. In particular, the FTC explained that the "stipulated order" (by means of which the settlement was concluded) provides for a forward-looking prohibition of misrepresenting, among others things, the company's participation in the Privacy Shield, as well as the extent to which it complies with its Principles. In this respect, a number of questions were raised by the EU delegation about the

[34] See points 145-147 of the adequacy decision.
[35] FTC Press release https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations
[36] FTC Press release https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc
[37] FTC Press release https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related
[38] FTC Press release https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions

FTC's complaint, as it does not refer to potential Privacy Shield (or Safe Harbor) violations, even though the described behaviour seems to correspond to substantive violations of the framework.[39] The FTC explained that the processing operations that were addressed in the complaint (and which involved a direct interaction with consumers) are not covered by Facebook's limited Privacy Shield certification (which is restricted to two B2B products where Facebook is a subprocessor). In order to have a complete overview of Facebook's privacy practices *vis-à-vis* its users, it would then be necessary to also look at the outcome of enforcement action in the EU. Moreover, the FTC provided reassurance that the "immunity" granted to Facebook as part of the settlement[40] does not cover possible future enforcement action under the Privacy Shield (relating to violations that would have taken place during the period covered by the settlement or any subsequent actions), as the complaint did not concern processing operations covered by Facebook's certification.

At the same time, the FTC clarified that, had Facebook's activities been covered by its Privacy Shield certification, they would have amounted to substantive violations of the framework. In this respect, the DoC informed during the annual review meeting that it had sent a Compliance Questionnaire to Facebook to further investigate its compliance with the framework (see above, Section 4.1.2).[41]

With respect to more general developments, the FTC provided an update during the annual review meeting on the outcome of the reflection process launched last year on "Competition and Consumer Protection in the 21st century" with respect to its current powers to deter unfair and deceptive practices in privacy and data security matters. The FTC explained that a number of issues were addressed in the course of a series of public hearings that were held by the FTC in autumn 2018 and spring 2019 in which the FTC looked at the effectiveness of its current remedial authority. The FTC still has to decide on the concrete output that will follow from these hearings, which might for example take the form of reports, recommendations for its own practices or recommendations to Congress. The Commission services remain very interested in the outcome of this process and will continue to follow it closely.

4.1.4. Complaint handling

Pursuant to the Privacy Shield, individuals can first of all address any complaints regarding compliance with the Privacy Shield Principles to the companies concerned. They have the right to have these complaints addressed within 45 days, if necessary by a decision providing for an effective remedy. Companies have created dedicated mechanisms to handle complaints and requests, and as confirmed by the responses received to the Commission's questionnaire, the majority of complaints and requests from individuals to companies are successfully

[39] See https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_complaint_filed_7-24-19.pdf.
[40] The Order provides that the settlement resolves "any and all claims of violations" of the 2012 Order, as well as "all consumer-protection claims known by the FTC prior to 12 June 2019".
[41] If the DoC finds that there is credible evidence that a company does not comply with its commitments, it sends a Compliance Questionnaire to which the company is required to respond within 30 days. If there is no timely and satisfactory response, this may ultimately lead to a removal of the company from the framework. See also Section 4.1.2, p. 9 of the Commission's Staff Working Document on the second annual review.

handled through these mechanisms, within the required timeline and to the satisfaction of both sides.[42]

4.1.4.1. Independent Dispute Resolution Mechanisms (IRMs)

In terms of structural developments concerning complaint handling and annual reporting by independent dispute resolution providers, the Commission services noted at the third annual review that in an effort to harmonize the annual reports issued by those providers and as recommended by the Commission during the second annual review,[43] the DoC had updated its guidance to IRMs in July 2019, setting out a number of standard elements that providers have to include in their reports.[44] Those elements were indeed included in the annual reports of IRMs covering the reporting period 1 August 2018 to 31 July 2019.

Moreover, the DoC's guidance requires those IRMs that offer both dispute resolution services and external compliance verification services to describe in their annual reports how they avoid any actual or potential conflicts of interest in situations where they provide a company with both verification and dispute resolution services. Out of nine IRMs in total, three provide both dispute resolution and verification services.[45] Further to the DoC's updated guidance, all of these have adressed conflicts of interest in their latest annual reports. Conflicts of interests are avoided by relying on seperate teams/analysts to work on dispute resolution on the one hand and verification on the other hand, by restricting access to data under each function to the relevant team members, and by introducing a separate managing and reporting structure.

The number of complaints received by IRMs in the third year of operation of the Privacy Shield is higher compared to the first and second year of operation of the Privacy Shield.[46] However, as it was the case in previous years, the large majority of complaints were ineligible, as they were not addressed to the IRM chosen by the company concerned or they did not concern data that had been transferred under the Privacy Shield (i.e. relating to companies that are not certified under the Privacy Shield or complaints coming from individuals in the U.S.). In total, IRMs received 48 eligible complaints (compared to 38 eligible complaints in the previous reporting period). All of them were resolved in a timely manner and to the satisfaction of the EU data subject. The majority of complaints were related to requests to correct or delete personal data, to unsubscribe, to reactivate disabled accounts and to contact a company representative.

[42] Companies report to have received a number of requests from individuals concerning access, correction or deletion of personal data, which were swiftly resolved.
[43] See Section 4.1.4.2 of the Commission Staff Working Document on the second annual review, p. 16.
[44] These standard elements include, for example, the period covered in the report, the number of companies enrolled in the dispute resolution program, whether the IRM also provides Privacy-Shield related verification services and if that is the case, the number of companies that receive both dispute resolution and verification services, a description of the IRM's complaint eligibility requirements and its complaint review process, and statistics for Privacy Shield-related complaints received during the reporting period, including the number and types of complaints, the measures taken and the outcome of the complaints.
[45] VeraSafe, TrustArc and PrivacyTrust.
[46] See Section 4.1.3.2 of the Commission Staff Working Document on the first annual review and Section 4.1.4.2 of the Commission Staff Working Document on the second annual review.

More specifically, Better Business Bureau (BBB) received 1053 complaints (compared to 525 complaints in the previous year), with 200 originating from the EU and Switzerland.[47] The majority of these complaints was directed either at companies that had not chosen BBB as IRM or were not Privacy Shield-certified. Eight complaints were ultimately found eligible. While in five of these cases the complaint was dropped by the complainant following requests for additional information, the remaining three complaints led to the opening of cases. All of these cases involved the Privacy Shield's Access Principle,[48] one case also involved the improper handling of information. All cases were successfully resolved; access was granted and in one case personal data was also deleted at the request of the complainant, while in another case the complaint also led to a change in business practices.

As another example, TrustArc handled 38 eligible complaints against Privacy Shield participants. The majority of complaints concerned account access/creation (6), changes to/deletion of personal data (11) and difficulties with unsubscribing (6). All complaints were resolved to the satisfaction of both sides, for example through the removal of personal data, through changes to the website or practices of the company, through the closing of accounts or through educational measures.

JAMS reported having received two eligible complaints under the Privacy Shield framework, one concerning a request to have personal data verified and the other one concerning a request to have personal data deleted. Both complaints were successfully resolved by facilitating communication between the company and the complainant and monitoring until the complainant had received a satisfactory response.

Other IRMs have either not received any complaints, or, if complaints were received, these were found to be ineligible, because they contained an incoherent claim, did not come from EU individuals, or were not related to the Privacy Shield.

The Commission services welcome that an increasing number of EU data subjects is making use of their rights under the Privacy Shield, which shows that there is an increasing awareness of the individual rights guaranteed under the Privacy Shield, as well as of privacy rights more generally.

[47] More than 1000 Privacy Shield certified companies are enrolled with BBB.

[48] Under the Access Principle, individuals have the right to obtain from an organisation confirmation of whether or not the organisation is processing personal data relating to them, have communicated such data to them to verify its accuracy and the lawfulness of the processing, and have the data corrected, amended or deleted where it is inaccurate or processed in violation of the Principles, see Principle 8, Annex II to the adequacy decision.

4.1.4.2. The Binding Arbitration Mechanism

The arbitration panel continues to be fully operational. A pool of arbitrators has been established and while one of the selected arbitrators had to step down from his function in the past year,[49] the remaining pool is sufficient to fulfil the requirements of the Privacy Shield.[50]

Interestingly, in the Privacy Shield's third year of operation the Binding Arbitration Mechanims has been triggered for the first time. One request was submitted in January and another one in April 2019. Both requests were inadmissible. In the first case, the complainant had not completed the steps that are required to be taken prior to iniating an arbitration claim.[51] In the second case, the request concerned a company that was not certified under the Privacy Shield.

The fact that the Arbitration Mechanism has eventually been invoked seems to confirm the growing interest and awareness of individuals in the EU with respect to their rights under the Privacy Shield and/or privacy matters more generally (see above, Section 4.1.4.1). Yet the two cases, as well as the above findings concerning the complaints received by IRMs, also highlight the need to better inform individuals in the EU about the mechanisms available under the Privacy Shield and the respective requirements for successfully invoking them. The Commission services call on the data protection authorities to continue and even intensify their efforts in this regard. The Commission services will also look at ways to further improve the understanding of EU individuals on how to invoke their rights under the Privacy Shield.

4.1.5. Automated individual decision-making

At the last annual review Commission services concluded that there was little evidence that Privacy Shield-certified companies were engaging in automated decision-making on the basis of personal data transferred under the Privacy Shield (as opposed to decisions taken on the basis of data collected in the context a direct relationship between a U.S.-based company and customers in the EU, which are generally directly subject to the GDPR and its specific protections on automated decision-making). At the same time, the Commission services noted that since automated decision-making is a rapidly evolving area, it continues to require close monitoring in the context of future reviews.[52]

The input received in preparation of this year's annual review from trade associations whose members are Privacy Shield-certified confirmed that the number of Privacy Shield participants that use data transferred under the Privacy Shield to carry out automated forms of decision-making continues to be limited and generally does not seem to relate to decisions

[49] The arbitrator concerned was appointed as a member of the independent Privacy and Civil Liberties Oversight Board (PCLOB) in June 2019.
[50] Initially, a pool of 23 arbitrators had been established and two arbitrators have since then stepped down. The Privacy Shield requires a pool of at least 20 arbitrators; see Annex 2 to ANNEX I of the adequacy decision.
[51] An individual is required to (1) raise the claimed violation directly with the organization; (2) make use of the independent recourse mechanism; and (3) raise the issue to the DoC, through the competent Data Protection Authority. See Annex I to ANNEX II of the adequacy decision.
[52] See Section 4.1.5 of the Commission Staff Working Document on the second annual review.

that produce a legal or similarly significant effect on individuals. Trade associations explained that to the extent some form of automated decision-making takes place, it is mainly carried out for (i) offering personalised advertising or services, (ii) detecting fraud, (iii) preventing cyber threats, and for (iv) HR related purposes. In these situations companies provide users with details about the information collected and how it is used, as well as with key controls for managing their privacy settings, including a right to intervention.

It is worth noting thatautomated decision-making was one of the topics addressed in the context of the series of public hearings that were held by the FTC in autumn 2018 and spring 2019 on Competition and Consumer Protection in the 21st century, in which the FTC looked at the effectiveness of its current remedial authority.[53] Among others, the hearings covered algorithms, artificial intelligence, and predictive analytics as well as privacy, big data, and competition. The FTC still has to decide on the concrete output that will follow from these hearings, which might for example take the form of reports, recommendations for its own practices or recommendations to Congress. The Commission will continue to follow this process with great interest.

Finallly, the Commission services welcome that as a member of the OECD the U.S. approved the OECD Principles on Artifical Intelligence (AI) in May 2019.[54] These Principle set strong standards around notions such as transparency, explainability and challengeability and show that the EU and the U.S. tend to converge on the way certain fundamental questions relating to AI should be addressed. They notably require that AI systems should be designed in a way that respects the rule of law, human rights, democratic values and diversity; should include appropriate safeguards to ensure a fair and just society, for example by enabling human intervention where necessary, and should allow for transparency and responsible disclosure to ensure that people understand AI-based outcomes and can challenge them.[55]

4.1.6. Human resources data

At the first annual review, it had emerged that there is a different reading of the notion of HR data by the DPAs on the one hand and the DoC on the other.[56] According to the DoC, only the transfer of human resources data in the context of the employment relationship alls within the category of HR data under the Privacy Shield. The DPAs instead were of the opinion that

[53] See https://www.ftc.gov/policy/hearings-competition-consumer-protection.

[54] See https://www.oecd.org/going-digital/ai/principles/. While OECD Recommendations are not legally binding, they are highly influential. They have set the international standard in a wide range of areas and helped governments design national legislation.

[55] See in particular "Section 1.3.Transparency and explainability
AI Actors should commit to transparency and responsible disclosure regarding AI systems. To this end, they should provide meaningful information, appropriate to the context, and consistent with the state of art:
i.to foster a general understanding of AI systems,
ii.to make stakeholders aware of their interactions with AI systems, including in the workplace,
iii.to enable those affected by an AI system to understand the outcome, and,
iv.to enable those adversely affected by an AI system to challenge its outcome based on plain and easy-to-understand information on the factors, and the logic that served as the basis for the prediction, recommendation or decision."

[56] See report of the Article 29 Working Party on the EU-U.S. Privacy Shield – First annual Joint Review, adopted on 28 November 2017, p. 9.

all data concerning an employee collected by the EU company in the context of an employer-employee relationship should be considered HR data, irrespective of whether the data is transferred within a corporate group or to a different commercial operator.[57]

The notion of human resources data was thus mentioned by the Commission in its report on the first annual review as a concept that would benefit from additional clarification. At the second annual review meeting, the DoC, the FTC and the DPAs continued their discussion about the differences in interpretation of the framework and the consequences for the applicable safeguards. The Commission services noted that they made progress in understanding each other's position and urged the EU and U.S. enforcers to continue their constructive dialogue with a view to issuing common guidance on this important topic.

Although at the time of the third annual review some contacts had taken place between DPAs on the one hand and FTC and DoC on the other hand, these contacts had occurred very late in the year and had not yet led to any concrete outcome. These contacts had helped to further improve the mutual understanding of the questions at stake and both sides have agreed that in order to advance on these questions, it would be useful to collect the views of stakeholders to better identify the scenarios involving the transfer of HR data under the Privacy Shield. There was also a common understanding that certain protections under the Privacy Shield, e.g. with respect to retaliation against employees, are not relevant in a situation where HR data is transferred to a company that is not the employer of the individuals concerned.

While the Commission services welcome that the discussion has continued and further progress has been made, they regret that the DoC did not take the initiative to contact the DPAs earlier. As reported by DPAs, companies both in the EU and in the U.S. frequently enquire about the definition and treatment of HR data under the Privacy Shield. There is therefore a pressing need for further guidance. The DPAs have a key role in enforcing the Privacy Shield requirements with respect to HR data and are thus best placed to contribute to this guidance. On that basis, the Commission services expect common guidance to be issued in the coming months.

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

In the Privacy Shield's third year of operation, the public debate with respect to the privacy legal framework in the U.S. has continued. This debate was sparked last year by scandals involving the extensive sharing of personal data and significant data breaches affecting a high number of users both in the U.S. and worldwide. It has lead to an increased legislative activity at State level, as more than ten States have adopted or are considering to adopt privacy laws. Moreover, the number of federal privacy bills that have been proposed in Congress has multiplied, although timeline and outcome are currently still unclear.[58] Yet it is clear that there is real momentum for federal privacy legislation in the U.S., and as this is of

[57] Report of the Article 29 Working Party of 28 November 2017 on the EU-U.S. Privacy Shield – First annual Joint Review, p. 9.

[58] Some of these bills share certain commonalities with the EU data protection framework. For an overview of different initiatives, see for example https://www.epic.org/GradingOnACurve.pdf.

direct relevance for the functioning of the Privacy Shield framework, the Commission services look forward to further engaging with the U.S. authorities on the ongoing initiatives and will continue to follow them closely. It is through such an approach, based on comprehensive privacy legislation, that convergence across the Atlantic can be achieved in the longer term to the benefit of EU and U.S. businesses and consumers alike, which would also strenghten the foundations on which the Privacy Shield framework has been developed.

A further interesting development is the Privacy Framework being developed by the National Institute of Standards and Technology (NIST) in collaboration with industry, civil society, academia, federal agencies, etc,. which was released as a preliminary draft for public comments just before the third annual review meeting.[59] The Framework will be a voluntary tool that will help companies to strengthen their privacy policies and to introduce mechanims that would facilitate the exercise of certain individual rights. Further to the consultation of stakeholders, NIST will develop a new version of the Framework by the end of the year.

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

With respect to the access to and use of personal data transferred under the Privacy Shield, the third annual review was first of all aimed at assessing whether all the limitations and safeguards that the adequacy decision relies on remain in place. It was also intended to receive clarifications on certain aspects of the implementation of these limitations and safeguards, including in light of any new developments that may have taken place. This concerns not only the legal framework for the collection of intelligence information, i.e. the relevant statutes, Presidential Policy Directives, Executive Orders and agency rules and procedures, notably the targeting and minimisation procedures adopted under the Foreign Intelligence Surveillance Act (FISA), but also the oversight structure and the avenues for individual redress. At the same time, the third annual review provided also an opportunity to further clarify certain aspects of the legal framework, the functioning of different oversight mechanisms and the possibilities for redress, notably in light of the questions that were raised in the context of the litigation relating to the Privacy Shield that is currently pending before the Court of Justice of the European Union.[60]

4.2.1. Relevant developments and clarifications with respect to the U.S. legal framework

At the third annual review, the U.S. authorities explained and explicitly confirmed that the U.S. legal framework governing the collection and use of foreign intelligence information consists of a number of different instruments, all of which have the force of law in the U.S.

[59] See https://www.nist.gov/privacy-framework.

[60] See case T-738/16 La Quadrature du Net v. Commission. Questions on the Privacy Shield have also been raised in the context of case C-311/18 Data Protection Commissioner and Facebook Ireland, Maximilian Schrems ("*Schrems II*"), in which a hearing took place before the Grand Chamber of the Court of Justice on 9 July 2019.

legal system. This includes statutes such as FISA, but also Executive Orders, Presidential Policy Directives, agency rules such as the targeting procedures, and orders of the Foreign Intelligence Surveillance Court (FISC).

4.2.1.1. Section 702 FISA

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

As set out in the adequacy decision[61] and confirmed by the first and second annual review,[62] once personal data has been transferred to Privacy Shield-certified companies, U.S. intelligence authorities may compel the companies to disclose the data for national security purposes only on the basis of FISA or one of the statutes that authorise the use of so-called National Security Letters (NSLs).

Due to the conditions and limitations contained in these statutory authorisations for surveillance (which are described in the adequacy decision and the Commission Staff Working Document on the first annual review),[63] the collection of personal data on the basis of FISA or in the context of NSLs is always targeted.[64]

The U.S. authorities used the occasion of the third annual review to provide further clarifications on the way in which the collection of intelligence information is targeted under the intelligence programs carried out pursuant to Section 702 FISA (i.e. Prism and Upstream), and notably on the choice of selectors that are used to target this collection.

Section 702 FISA allows the targeting of non-U.S. persons reasonably believed to be located outside the United States to acquire foreign intelligence information.[65] This targeting is carried out by identifying so-called selectors, which identify a specific communication account, e.g. a telephone number or an email address. Selectors are therefore never key words or names of persons.[66]

[61] Recital 78 of the adequacy decision.
[62] See Section 4.2.1.2 of the Commission Staff Working Document on the first annual review and Section 4.2.1 of the Commission Staff Working Document on the second annual review.
[63] See recitals 71, 78-81 and sections 4.2.1.2 and 4.2.1.3 of the Commission Staff Working Document on the first annual review.
[64] Outside of the territory of the U.S., the collection of personal data "in bulk" can exceptionally take place on the basis of Executive Order (E.O.) 12333 where targeted collection is not feasible. The collection of personal data for national security purposes from companies that have received such data under the Privacy Shield framework, however, cannot be based on E.O. 12333. Bulk collection does therefore not occur with respect to data received under the Privacy Shield.
[65] 50 U.S.C. § 1881a(a), recital 109 of the adequacy decision. Foreign intelligence information is defined in Section 101(e)(50 U.S.C. 108).
[66] See recital 82 of the adequacy decision.

The NSA, which is the intelligence agency responsible for the targeting under Section 702 FISA, chooses a certain communication account as selector if it has determined on an individualised basis that a (1) non-U.S. person, that is (2) reasonably believed to be located outside the United States (3) will use the selector to communicate or receive foreign intelligence information.[67] The method for determining that these three requirements are fulfilled and thus for choosing the selectors is governed by the targeting procedures, which are binding on the authorities carrying out the surveillance, are approved by the FISC and subject to its judicial review.[68] As set out in the NSA's targeting procedures, the NSA can only direct surveillance at a target when it has already learned something about the target.[69] Section 702 targeting thus begins notably when an analyst identifies or is informed of a foreign intelligence lead, i.e. information indicating that a particular person may possess or receive the types of foreign intelligence information sought.[70] This information may come from different sources, for instance from human intelligence. Through these other sources, the analyst must also learn about a specific selector (i.e. communication account) used by the potential target. The analyst must then come to the reasonable conclusion, based on the totality of circumstances, that the target is expected to possess, receive, and/or is likely to communicate foreign intelligence information. This assessment must be particularized and fact-based, informed by analytic judgment, the specialized training and experience of the analyst, as well as the nature of the foreign intelligence information to be obtained.[71] The NSA targeting procedures include a list of factors that the NSA will consider in determining whether the choice of a certain selector will be likely to result in the collection of the

[67] 50 U.S.C. § 1881a(a), Procedures used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended, of March 2018 (NSA targeting procedures), available at https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_NSA_Targeting_27Mar18.pdf, p. 1-4, further explained in PCLOB report, p. 41-42.

[68] In order to collect foreign intelligence information pursuant to Section 702 FISA, the Attorney General and the Director of National Intelligence submit annual certifications to the FISC which authorize the targeting of non-U.S. persons reasonably believed to be located outside the United States to acquire certain categories of foreign intelligence information. Among others, the certifications must contain "targeting procedures" approved by the Attorney General, see U.S.C.A. § 1881a(h). The FISC reviews the certifications and the related procedures, including the targeting procedures, for compliance with the requirements of FISA, see U.S.C.A. § 1881a(j) If the requirements are fulfilled, the FISC approves the certifications and the use of the procedures for the collection of the foreign intelligence information specified in the certification, see U.S.C.A. § 1881a(j)(3). If it considers that the requirements are not fulfilled, the FISC can deny the certification in full or in part and request the procedures to be amended, see e.g. FISC Opinion of 18 October 2018, available at https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, as confirmed by the Foreign Intelligence Court of Review in its Opinion of 12 July 2019, available at https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf. Individual targeting determinations made under the targeting procedures are not reviewed by the FISC, but are subject to strict internal oversight. See PCLOB Report on the Surveillance Program Operated Pursuant to Section 702 FISA, July 2, 2014, available at https://www.pclob.gov/library/702-Report.pdf, p. 41-42.

[69] NSA targeting procedures, p. 2.

[70] PCLOB report, p. 42-43.

[71] NSA targeting procedures, p 4.

category of foreign intelligence information identified in one of the Section 702 certifications.[72]

Furthermore, the NSA targeting procedures require that analysts provide a written explanation of the reasons for their assessment that, at the time of the targeting, the target possesses, is expected to receive, and/or is likely to communicate foreign intelligence information.[73] The determinations made, including the written explanations, are documented in the relevant NSA database, where they are reviewed by two different senior NSA analysts to ensure that they meet all the requirements of the targeting procedures.[74] This written justification is later reviewed for compliance with the targeting procedures. Such compliance review is carried out on a bimonthly basis by officials at intelligence oversight offices at the Department of Justice and the Office of the Director of National Intelligence, who are obliged to report any violation to the FISC and to Congress.[75]

The Commission services welcome these clarifications, which confirm the Commission's findings in the adequacy decision that the collection of foreign intelligence information under Section 702 FISA is targeted through the use of selectors and that the choice of selectors is governed by law, subject to independent judicial and legislative oversight.

4.2.1.2. Presidential Policy Directive (PPD)-28

At the third annual review meeting, the U.S. authorities, represented by the ODNI, explicitly confirmed that PPD-28 remains in full force and effect and has not been subject to any amendments. There have also been no modifications to the procedures implementing PPD-28 within the different elements of the Intelligence Community.

[72] PCLOB report, p. 45. See also Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence, Reporting Period: December 1, 2016 – May 31, 2017, p. 41 (October 2018), available at: https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

[73] NSA targeting procedures, p. 8.

[74] PCLOB report, p 46. Failure to provide a written justification constitutes a documentation compliance incident that is reported to the FISC and Congress. See Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence, Reporting Period: December 1, 2016 – May 31, 2017, p. 41 (October 2018), available at https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

[75] PCLOB report, p. 70-72; Rule 13(b) of the Rules of Procedure of the United States Intelligence Surveillance Court, available at https://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf. For example, a recent joint DOJ/ODNI assessment discusses the misapplication of the "foreign intelligence" requirement caused by one targeting office's misunderstanding of the targeting procedures. That office erroneously chose certain communication accounts as selectors without having sufficient information to assess whether the users of the accounts would possess, receive or communicate the category of foreign intelligence information authorised under the relevant Section 702 certification. Remedial action was taken, notably additional training and guidance to all NSA personnel on the requirements of the targeting procedures. Moreover, any data collected because of such errors has to be deleted. See Semiannual assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence, Reporting Period: June 1, 2015 – November 30, 2015, p. 35-36 and 43 (November 2016). Available at https://www.dni.gov/files/documents/icotr/15th-702Joint-Assessment-Nov2016-FINAL-REDACTED1517.pdf.

This is an important piece of information, as the protections of PPD-28 apply to all signals intelligence activities of the Intelligence Community. With respect to the collection of foreign intelligence information under FISA and thus within the territory of the United States,[76] the relevant limitations and safeguards are first and foremost provided by the FISA statute itself. However, PPD-28 also has a certain role, as it extends specific protections under FISA to foreigners which would otherwise be limited to U.S. persons only. In particular, PPD-28 extends to non-U.S. persons the protections provided for U.S. persons with respect to the retention and dissemination of data.[77]

Moreover, in light of the questions asked during the hearing before the Court of Justice of the European Union in the so-called *Schrems II* case, the U.S. authorities used the third annual review meeting as an opportunity to further clarify that the provisions on bulk collection in PPD-28, including those on temporary acquisition,[78] do not apply to the collection of foreign intelligence information within the U.S. (for example, to the collection of information from a certified company processing data transferred from the EU under the Privacy Shield), such as collection carried out under Section 702 FISA under the Prism or the Upstream program, as this collection is always targeted.[79]

4.2.1.3. The re-authorization of Section 501 FISA

Section 501 FISA (formerly Section 215 of the USA PATRIOT Act of 2001) authorizes the Federal Bureau of Investigation (FBI) to access and collect any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person. Following the enactment of the USA FREEDOM Act in 2015, bulk collection is expressly prohibited under Section 501 FISA. Instead, Section 501 FISA now allows the collection of records (in particular telephone metadata and business records) based on a specific selection term for which there is

[76] As set out in the adequacy decision and confirmed by the first and second annual reviews, once personal data has been transferred to Privacy Shield-certified companies, U.S. intelligence authorities may compel the companies to disclose the data for national security purposes only on the basis of FISA or on the basis of one of the statutes that authorise the use of NSLs. Due to the conditions and limitations contained in these statutory authorisations, the collection of personal data within the U.S. is always targeted. See Section 4.2.1. of the Commission Staff Working Document on the second annual review and Section 4.2.1.2 of the Commission Staff Working Document on the first annual review.

[77] The protections of PPD-28 have even more relevance for the collection of intelligence information for national security purposes under Executive Order (E.O.) 12333, which only takes place outside of the territory of the U.S., i.e. not from companies processing personal data in the U.S. that they have received under the Privacy Shield framework.

[78] Section 2 of PPD-28 contains limitations on the use of signals intelligence collected in bulk (as explained in this Commission Staff Working Document, data received by Privacy Shield-certified companies cannot be collected in bulk and even outside the U.S. bulk collection may take place only where targeted collection is not feasible, for instance for technical reasons). In this respect, Section 2 sets out that if signals intelligence information is collected in bulk, the use of this information is restricted to six specific purposes. The first sentence of footnote n°5, which refers to Section 2, specifies that these use limitations do not apply to signals intelligence data that is temporarily acquired to facilitate targeted collection. In this scenario, the only purpose of the collection, and therefore the exclusive use of the data collected, is the further selection of specific information by applying a specific identifier or selection term. The limitation to the six purposes contained in Section 2 is therefore not relevant. In such a scenario, only data that responds to the application of a certain discriminant is inserted into government databases, while the remaining data is destroyed.

[79] See Commission Staff Working Document on the second annual review, Section 4.2.1.

reasonable suspicion that it is associated with international terrorism, as approved by the FISC.[80]

Some provisions of the USA FREEDOM Act are scheduled to expire on 15 December 2019 unless they are re-authorized by Congress,[81] among which the authority originally provided by section 501 FISA and subsequently modified by the USA FREEDOM Act that allows the FBI to obtain certain business records in a national security investigation, as well as the call detail records program undertaken by the NSA. During the third annual review, it was clarified that, due to the limited practical value of information obtained through the call detail records program and a certain number of compliance incidents in relation to this program, the NSA had decided to suspend the call detail records program and had deleted all the data acquired under this authority. The ODNI specified that, despite the limited value of the authority and the fact that it is currently not used, the government intends to seek re-authorization, in case it should become relevant again in the future.

The Commission services stress the importance of ensuring that, in case of re-authorization, the existing limitations and safeguards to this authority (such as the prohibition of bulk collection) remain in place and that the scope of this authority is not broadened. The Commission services will closely monitor any developments in this regard.

Finally, the Commission services note that the safeguards introduced by the USA FREEDOM Act that the Privacy Shield adequacy decision relies on and that are thus particularly relevant for its correct functioning (notably the possibility for companies to report on the aggregate number of access requests received from U.S. public authorities, the possibility for the FISC to appoint an outside lawyer as an independent advocate on behalf of privacy as *amicus curiae* in cases that present novel or significant legal issues, as well as increased transparency obligations for the Intelligence Community more generally with the requirement for the U.S. government to publicly release FISC decisions concerning significant interpretations of law and statistical reporting) are not expiring at the end of the year.

4.2.1.4. Surveillance activities in practice: figures and trends

The ODNI's Statistical Transparency Report Regarding Use of National Security Authorities for calendar year 2018 shows that the number of targets under Section 702 FISA increased from 129,080 in CY2017 to 164,770 in CY2018. Conversely, the number of NSLs issued decreased from 12,762 in CY2017 to 10,235 in CY2018.

[80] See 6th annual Statistical Transparency Report Regarding Use of National Security Authorities (dated 2019 for calendar year 2018), pp. 25-31. Released April 30, 2019, and available at: https://www.dni.gov/files/CLPT/documents/2019_ASTR_for_CY2018.pdf.

[81] Namely these four provisions are expiring: (1) the "lone wolf" authority allowing surveillance of a suspected terrorist who is inspired by foreign ideology but is not acting at the direction of a foreign party, (2) the roving wiretap authority which allows the U.S. government to collect intelligence on a target who seeks to thwart surveillance by, for example, cycling through cell phones, , (3) the authority to allow the FBI to obtain certain business records in authorized national security investigations and (4) the call detail records program undertaken by the NSA (Section 705 of the USA FREEDOM Act).

In addition, as allowed under the USA FREEDOM Act,[82] several Privacy Shield-certified companies have published transparency reports which inform about the number of FISA and NSL access requests they have received during a given reporting period. These companies include for instance Snap Inc., Google, Facebook, Twilio, Reddit, Dropbox, LinkedIn, Pinterest, Uber and Twitter.

When compared with last year's figures[83], the numbers published by companies mirror the developments presented in ODNI's Statistical Transparency Report. For example, during the reporting period January 2018 to June 2018, Google received between 500 and 999 requests for access to content under FISA, affecting between 97 000 and 97 499 users, and between 3 and 499 NSL requests, affecting between 1000 and 1499 users.[84] Facebook received between 0 and 499 requests for access to content under FISA, affecting between 69 000 and 69 499 accounts, during the reporting period January to June 2018.[85] From July to December 2018, Facebook received between 0 and 499 NSL requests, affecting between 0 and 499 accounts.

At the third annual review meeting, the U.S. authorities explained that the number of targets under the different legal authorities for the collection of foreign intelligence information typically fluctuates from year to year. Reasons for these fluctuations are changes in the intelligence community's operational priorities, changes in the use of technologies and means of telecommunication as well as changing target behaviour more generally.

4.2.2. Independent oversight and redress

4.2.2.1. The Privacy and Civil Liberties Oversight Board

At the time of the second annual review, the PCLOB consisted of three members, while two additional members had been nominated, but were awaiting confirmation by the Senate.[86] On 27 June 2019, the Senate confirmed Aditya Bamzai and Travis LeBlanc to be members of the PCLOB. In addition, the re-nomination of Board Member Edward Felten was confirmed for a six-year term.[87] With these confirmations, the PCLOB has a full slate of five Members for the first time since 2016. The Commission services welcome that the PCLOB has been reinstated to its full capacity and is now entirely operational.

Chairman Adam Klein and Member Travis LeBlanc participated in person in the third annual review meeting. They explained that, since the PCLOB regained quorum, its staff has more than doubled and seven new oversight projects have been initiated. The PCLOB is currently working on a total of ten oversight projects and on several advice projects, i.e. on more projects than ever before. In order to ensure maximum transparency of its work, the PCLOB

[82] USA FREEDOM Act of 2015, Pub. L. No 114-23, Section 602(a), 603(a), codified in FISA at 50 U.S.C. § 1874.
[83] See Section 4.2.1.2 of the Commission Staff Working Document on the second annual review.
[84] https://transparencyreport.google.com/user-data/us-national-security?hl=en.
[85] https://govtrequests.facebook.com/government-data-requests/country/US
[86] See Section 4.2.1.3.2 of the Commission Staff Working Document on the second annual review.
[87] The initial term of Edward Felten expired in January 2019, after which he was re-nominated.

published an inventory of active oversight projects as well as of other initiatives on its website in July 2019.[88]

Several of the ongoing oversight projects are particularly relevant for the Commission's periodic review of the Privacy Shield, as they concern the procedures and safeguards applying to government access to personal data of non-U.S. persons. In particular, the Board is reviewing the FBI's querying of data obtained under Section 702 FISA, including the procedures and technology used to ensure compliance with the applicable legal framework. Another ongoing oversight project concerns the NSA's collection of call detail records under the USA Freedom Act of 2015, which is interesting in light of the fact that this authority is due to expire at the end of 2019 and reauthorisation has been sought by the Intelligence Community (see above, Section 4.2.1.3).

Moreover, it was confirmed during the third annual review meeting that the PCLOB is reviewing the implementation of the Board's recommendations from its reports on Section 702 and PPD-28.[89] This shows that the oversight carried out by the PCLOB is not limited to a one-off review, but is an ongoing exercise with continuous follow-up.

Finally, it was explained that the examination of certain counterterrorism-related activities conducted pursuant to EO 12 333 remains ongoing and that the Board is actively working on it.[90] However, no timeline was provided with respect to its finalization. The Commission services would welcome a quick finalisation of this work and expect that at least parts of the Board's report would be declassified.

4.2.2.2. The Privacy Shield Ombudsperson mechanism

At the time of the second annual review, the position of Under Secretary in the State Department to whom the office of the Ombudsperson has been assigned had not yet been filled by a permanent appointment. Although the acting Ombudsperson continued to carry out all relevant functions, the absence of a permanent appointee after two years of operation of the framework remained highly unsatisfactory. As a consequence, the Commission had called on the U.S. administration to confirm its political commitment to the mechanism by appointing a permanent Privacy Shield Ombudsperson as a matter of priority. To this end, the Commission voiced the expectation that the U.S. government would identify an appointee to fill the Ombudsperson position on a permanent basis by 28 February 2019.[91]

This first step was taken on 18 January 2019, when President Trump announced the nomination of Keith Krach as Under Secretary of State for Economic Growth, Energy and the Environment, to whom the office of the Ombudsperson has been assigned. On 20 June 2019, Mr. Krach was confirmed by the Senate, as the last step in the appointment procedure. The

[88] See https://www.pclob.gov/newsroom/20190708.html.
[89] See also Section 4.2.1.1.2 of the Commission Staff Working Document on the second annual review.
[90] In particular, the Board is still carrying out two "deep dive" reviews: concerning the NSA's use of XKEYSCORE as an analytical tool for counterterrorism purposes and its implications for privacy and civil liberties, and concerning a classified counterterrorism-related activity conducted by the CIA.
[91] See Commission report on the second annual review, p. 5-6.

Commission services welcome the appointment of Mr. Krach as Privacy Shield Ombudsperson, which ensures that the position is filled on a permanent basis. Mr. Krach participated in the third annual review and explained that he has all relevant tools at his disposal in his role as Privacy Shield Ombudsperson to ensure that complaints are investigated and addressed.

At the time of the second annual review, a first request to the Ombudsperson had been submitted to the Croatian DPA and the relevant checks were still ongoing. During the third annual review meeting, it was explained that the request had been referred to the Ombudsperson mechanism by the EU Centralised Body,[92] but the Ombudsperson mechanism had eventually found the request to be inadmissible, as it concerned a unique identifier (an e-mail account) that had been deleted in 2012, i.e. before the Privacy Shield Decision had entered into application. The Ombudsperson mechanism informed the EU Centralised Body accordingly, which in turn ensured that the complainant was informed of the outcome. Both the EDPB representatives present at the third annual review meeting and the Ombudsperson confirmed that all relevant steps of the procedure had been triggered and completed in a satisfactory and cooperative manner.[93] Moreover, both sides had agreed on the finding of inadmissibility of this particular case. At the same time, the EDPB representatives explained that, following the experience with the handling of the first complaint, the EU Centralised Body was considering to further streamline its internal procedure.

The successful processing of this first request is an important indication that the Ombudsperson mechanism can properly perform its functions. Yet the Commission services welcome that the EDPB is considering to further develop its internal processes in light of the experience with the first request. Discussions are also ongoing between the Ombudsperson and the EDPB on the use of the electronic platform through which individual complaints are channelled. While the first complaint was found inadmissible and could thus not be discussed in substance during the third annual review, the meeting provided an opportunity to further clarify the process in case there would be an admissible complaint. In particular, the U.S. authorities explained how the Ombudsperson would work with other independent oversight bodies to investigate and remedy violations.

More specifically, the Inspector General (IG) of the Intelligence Community,[94] Michael Atkinson, explained during the third annual review meeting that his office would systematically be informed of complaints submitted to the Ombudsperson mechanism and would carry out an independent assessment. This procedure was also followed with respect to the abovementioned request, after it had been submitted to the Ombudsperson mechanism by the EU Centralised Body. In this respect, the IG explained that he carried out an independent

[92] The EU Centralised Body, or EU Individual Complaint Handling Body, consists of the DPAs of France, Austria, Germany, Bulgaria and the UK, as designated by the EDPB.

[93] A request is filed with a national DPA, which refers it to the EU Centralised Body once the request is found complete. After an additional review by the EU Centralised Body, the complaint is transmitted to the Ombudsperson mechanism via a specific online platform created for this purpose. See also Section 4.2.1.4.1, p. 34 of the Commission Staff Working Document on the second annual review.

[94] See also Section 4.2.1.3.1, p. 31 of the Commission Staff Working Document, which explains the role and powers of the Inspector General of the Intelligence Community.

assessment of the complaint, and also came to the conclusion that no further action was required.

In addition, the U.S. authorities explained how a case would be resolved if the investigation of a complaint before the Ombudsperson would reveal a violation of the targeting and minimisation procedures under Section 702 FISA.[95] It was clarified that any such violation would be reported to the FISC,[96] which would carry out an independent review and, if necessary, order the relevant intelligency agency to take remedial action.[97] The remedies in question may range from individual to structural measures, e.g from the deletion of unlawfully obtained data to a change in the collection practice, including in terms of guidance and training for staff. Moreover, during its annual review of the Section 702 certifications, the FISC would consider this incident of non-compliance, as well as any other identified incidents, to determine if the submitted certifications complied with FISA requirements. If the FISC found that the government's certifications were not sufficient, including because of particular compliance incident such as an incident identified by the Ombudsperson, the FISC could issue a so-called "deficiency order" requiring the government to remedy the violation within 30 days[98] or requiring the government to cease or not begin implementing the Section 702 certification.

Finally, it was confirmed that, if a violation of U.S. law (including a violation of Executive Orders, Presidential Policies and agency rules and procedures, e.g. the targeting and minimisation procedures approved by the FISC) would be identified in the course of the review of a complaint to the Ombudsperson, unlawfully collected data would be purged from all government databases and any reference to that data would be removed from intelligence

[95] These procedures are part of the government's applications for annual certifications which are submitted to the FISC for review and authorisation and on which data collection under Section 702 FISA is based.

[96] See p. 4 of the Privacy Shield Ombudsperson Mechanism Unclassified Implementation Procedure, available at https://www.state.gov/wp-content/uploads/2018/12/Ombudsperson-Mechanism-Implementation-Procedures-UNCLASSIFIED.pdf, and Rule 13(b) of the Rules of Procedure of the United States Intelligence Surveillance Court.

[97] See FISC Memorandum Opinion and Order of 3 October 2011 as an example of a deficiency order in which the government was ordered to correct the identified deficiencies within 30 days. Available at https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf. See also FISC Judge Walton Letter to Senator Leahy, 29 July 2013, Section 4, p. 10 -11, available at https://fas.org/irp/news/2013/07/fisc-leahy.pdf. See also FISC Opinion of 18 October 2018, available at https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, as confirmed by the Foreign Intelligence Court of Review in its Opinion of 12 July 2019, available at https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf, in which the FISC *inter alia* ordered the government to comply with certain notification, documentation and reporting requirements towards the FISC.

[98] See FISC Memorandum Opinion and Order of 3 October 2011 as an example of a deficiency order in which the government was ordered to correct the identified deficiencies within 30 days. Available at https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf. See also FISC Judge Walton Letter to Senator Leahy, 29 July 2013, Section 4, p. 10 -11, available at https://fas.org/irp/news/2013/07/fisc-leahy.pdf. See also FISC Opinion of 18 October 2018, available at https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, as confirmed by the Foreign Intelligence Court of Review in its Opinion of 12 July 2019, available at https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf, in which the FISC *inter alia* ordered the government to comply with certain notification, documentation and reporting requirements towards the FISC

reports.[99] An individual in the EU would thus be able to obtain the deletion of his or her personal data if it was unlawfully collected and processed by the U.S. Intelligence Community.

The Commission services welcome the additional explanations provided during the third annual review, which demonstrate how cooperation between the different independent oversight bodies strengthens the efficiency of the Ombudsperson mechanism. This includes the systematic involvement of the independent Inspector General of the Intelligence Community in the review of complaints, as well as the judicial oversight carried out by the FISC, where competent, and legislative oversight carried out by Congress. Moreover, the Commission services welcome the confirmation that, if a complaint to the Ombudsperson would reveal a violation of U.S. laws (including Executive Orders, Presidential Policies and agency rules and procedures), all unlawfully collected data would be deleted from government databases and reports.

4.2.2.3. Judicial remedies available to EU individuals

As regards the redress possibilities identified in the adequacy decision[100] and further discussed during the first and second annual review,[101] new case law was issued during the third year of operation of the Privacy Shield.

First, the ruling in *Fazaga v. FBI*[102] clarified the procedure under FISA that applies when the U.S. government invokes the State secrets evidentiary privilege (which allows the government to withhold evidence from litigation where disclosure would create an unacceptable risk of harm to national security). In particular, the Court of Appeal of the Ninth Circuit held that the procedure under FISA that provides for judicial review of secret evidence (50 USC §1806(f)) takes precedence over the State secrets evidentiary privilege. As a consequence, in cases involving alleged State secrets and FISA claims, the government may not withhold privileged evidence from the litigation and must instead submit that evidence to the court for *in camera* and *ex parte* review. This ensures independent judicial review of information obtained through electronic surveillance under FISA, including in situations where it could otherwise be withheld by the government on national security grounds.[103]

While the ruling contributes to ensuring that individuals benefit from judicial review of evidence obtained through electronic surveillance, including when it is used against them in

[99] See e.g. Semiannual assessment of compliance with procedures and guidelines issued pursuant to Section 702 of the Foreign Intelligence Surveillance Act, submitted by the Attorney General and the Director of National Intelligence, Reporting Period June 1, 2015 – November 30, 2015, first paragraph on p. 43, available at https://www.dni.gov/files/documents/icotr/15th-702Joint-Assessment-Nov2016-FINAL-REDACTED1517.pdf.
[100] Recitals 111-124 of the adequacy decision.
[101] See Commission Staff Working Document on the first annual review, section 4.2.4.1., p. 32-33 and Commission Staff Working Document on the second annual review, section 4.2.1.4.2, p. 34-35.
[102] Fazaga v. FBI (916 F.3d 1202 (9th Cir. 2019), the Court of Appeal of the Ninth Circuit.
[103] See also recital 112 of the Adequacy Decision.

administrative or judicial proceedings,[104] the case had not become final at the time of the third annual review, as the court had been petitioned to rehear the case.

In another case (*Jewel v. National Security Agency*),[105] the district court used FISA's *in camera* and *ex parte* procedure (set out in 50 USC §1806(f)) to review the provided evidence, but eventually ruled in favour of the U.S. Government. This ruling has also been appealed. As both abovementioned decisions have been appealed, any further developments in this respect will therefore have to be closely monitored.

Second, the case of *ACLU v. National Security Agency* concerned a request under the Freedom of Information Act ("FOIA") seeking the disclosure of documents concerning the U.S. government's surveillance powers under EO 12 333.[106] The Court of Appeal upheld that the requested documents could not be disclosed, in accordance with exemptions provided under FOIA. In the input provided by NGOs in response to the Commission's questionnaire, questions were raised as regards the use of FOIA as a means to obtain information about the law and policy governing surveillance in the U.S. In this respect, the Commission services note that in any modern system of access to documents, it is not unreasonable that certain exceptions exist when it comes to disclosing government records. What matters is that an independent court can review the use of the exception by the intelligence community (and order disclosure in case of abuse), which is what happened in this particular case. Moreover, as confirmed in the adequacy decision, as well as the first and second annual review, FOIA is an important instrument used by individuals to seek access to records held by federal agencies that further contributes to transparency in the area of national security and has led to disclosures of important documents in the past.[107]

With respect to the issue of standing, the case *Wikimedia v. National Security Agency*[108] is still pending, although the U.S. authorities informed that a ruling is expected any day. The case concerns a challenge to the lawfulness of the Upstream program under Section 702 FISA under the Electronic Communications Privacy Act and the Administrative Procedures Act. It is based on publicly available information about how Section 702 FISA operates (including the PCLOB report) and Wikimedia's assertion that, given its large volume of global internet communications, it is extremely likely that some of its data has been intercepted through the

[104] Surveillance under Section 702 may be challenged when the government uses information obtained under Section 702 in a criminal or other proceeding against a person, of any nationality, a safeguard which has led to several court decisions upholding the legality of Section 702 surveillance. An additional safeguard requires the government to notify any person, including an EU citizen, who was targeted for surveillance under Section 702, or whose communications were subject to collection, if the government seeks to use the FISA evidence against them in a legal proceeding. The person's standing is established in such cases, and the person can seek to exclude the evidence on the grounds that the collection was unlawful—for example, because the collection violated the FISA statute or a particular FISA Court order. If the reviewing court determines the collection was unlawful, it must exclude the evidence.

[105] Jewel v. National Security Agency, N.D. Cal. April. 25, 2019.

[106] ACLU v. National Security Agency (925 F.3d 576 (2nd Cir. 2019)).

[107] Recitals 114, 133 of the Adequacy Decision, Commission Staff Working Document on the first annual review, Section 4.2.4.1, p. 32 and Commission Staff Working Document on the second annual review, Section 4.2.1.4.2, p. 34-35.

[108] 857 F.3d 193 (4th Cir. 2017), *Wikimedia Foundation v. National Security Agency*. See also Commission Staff Working Document on the first annual review, Section 4.2.4.1, p. 33-34.

Upstream program. The trial court granted the U.S. government's motion to dismiss for lack of standing, but the appellate court reversed that decision, finding that Wikimedia's allegations met the legal requirements of the standing doctrine. The case has been referred back to the trial court, which will determine its jurisdiction over the case based on an analysis of the underlying evidentiary record.

The Commission services continue to closely montior the evolving case law in the U.S., notably with respect to the issue of standing.