EUROPEAN
COMMISSION

Brussels, 19.12.2018
SWD(2018) 497 final

COMMISSION STAFF WORKING DOCUMENT
Accompanying the document

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}

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 second year of operation. The findings are based on information gathered from relevant stakeholders and the U.S. authorities both in the preparation and during the Annual Joint Review meetings held in Brussels on 18 and 19 October 2018. The findings have further been informed by a study commissioned by the Commission and 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 seven 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 Document from the first annual review in 2017.[2] All aspects of the functioning of the Privacy Shield are covered, also taking into account developments that took place since last year. For detailed explanations on the relevant Privacy Shield requirements and obligations for each of these aspects, the Commission services refer to the Staff Working Document on the first annual review.

2. THE FIRST 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 notably provides for an annual evaluation of all aspects of the functioning of the framework by the Commission.[4] 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

[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. It is the successor of the Article 29 Working Party that was created under Directive 95/46/EC.

[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

[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.

[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(2017611 final, see http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619

[6] See footnote 2.

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] to which this report refers in the relevant sections.

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

The first annual review focused on verifying that all components of the Privacy Shield framework as agreed between the EU and the U.S. were effectively in place. The second year of operation of the framework allowed to look closer into the functioning of these elements, also taking into account relevant developments in the U.S. legal system. A central element of the second annual review and of the Commission's assessment was the implementation of the Commission's recommendations from the first annual review.

On 12 July 2018, the Commission services sent questionnaires to ten trade associations in the U.S.[8] to collect input from those of their members that are Privacy Shield-certified. The questionnaires focused on the experience of Privacy Shield-certified companies with the day-to-day functioning of the framework and covered a wide range of issues relating inter alia to the (re)certification process, approaches to comply with the Privacy Principles, 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.[9] 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 August 2018. Throughout the entire preparatory phase, the Commission services had exchanges with trade associations, individual companies and NGOs to follow-up on the

[7] See Commission Report on the first annual review, p. 4-7.
[8] 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.
[9] 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.

input provided. This notably included a meeting on 20 September with industry and business associations and a meeting on 8 October with NGOs.

The Commission services also sent a detailed set of questions to the U.S. authorities that administer and oversee the Privacy Shield framework. On 16 October, the Commission services received written material from the U.S. authorities, including a summary of how the Commission's recommendations from the first annual review have been addressed. Earlier in 2018, the U.S. authorities informed the Commission services of developments relevant to the Privacy Shield, such as newly introduced monitoring and oversight mechanisms, appointments to key oversight and enforcement bodies and legislative developments.

In line with its recommendation from the first annual review, the Commission services commissioned a study on automated decision-making in early 2018. The Commission services received the final study on 8 October 2018.

Following the designation by the EDPB of its representatives to the annual review during the Plenary meeting in May 2018, the Commission services met with the representatives (on 5 September, 26 September and 17 October 2018) to prepare for the Annual Joint Review, discuss the input received and identify which aspects require additional information-gathering and clarification.

The Commission had several exchanges with the European Parliament, both at Committee (Committee on Civil Liberties, Justice and Home Affairs) and Plenary level. For example, Commissioner for Justice, Consumers and Gender Equality Jourová participated in the Plenary debate on 4 July 2018 on the (then) draft resolution on the Privacy Shield.[10] The resolution adopted by the Parliament constituted a key input for the second annual review.

The Commission also kept the EU Member States closely informed and received their feedback, notably in meetings of the Council Working Party on Information Exchange and Data Protection ("DAPIX") in July and the Article 93 Committee (established by the General Data Protection Regulation ("GDPR")[11]) in September 2018.

4. THE SECOND ANNUAL REVIEW – PROCESS AND FINDINGS

The second Annual Joint Review took place in Brussels on 18 and 19 October 2018. On the U.S. side, representatives from the Department of Commerce (the "DoC"), the Department of State, the Federal Trade Commission (the "FTC"), 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 (the "PCLOB")

[10] European Parliament Resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-U.S. Privacy Shield (2018/2645(RSP)), see http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0315+0+DOC+PDF+V0//EN

[11] See Article 93 of the Regulation (EU) 2016/679 of the European parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016, p.1.

participated in the review, as well as the acting Ombudsperson and the Inspector General for the Intelligence Community.

In addition, representatives from one of the organisations that offer independent dispute resolution services under the Privacy Shield and the American Arbitration Association provided information during the relevant review sessions. Finally, the review was informed by presentations by Privacy Shield-certified organisations[12] on how companies comply with the requirements of the framework.

The review was opened by the Commissioner for Justice, Consumers and Gender Equality Věra Jourová, U.S. Secretary of Commerce Wilbur Ross, the FTC Chairman Joseph Simons and the Chair of the European Data Protection Board Andrea Jelinek. It was conducted for the EU by representatives of the European Commission's Directorate General for Justice and Consumers. The EU delegation also included seven 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 on the first day and issues relating to government access to personal data on the second day.

4.1. COMMERCIAL ASPECTS

With respect to the "commercial aspects", the Commission focused the second review on recent developments in the administration and supervision of the framework, as well as its day-to-day functioning. This included the certification and re-certification process, oversight and enforcement, complaint handling and awareness-raising. In addition, the review looked at 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 first annual review and could be relevant for the functioning of the commercial aspects of the Privacy Shield.

4.1.1. The (re)-certification process

The first annual review focused on the procedures put in place by the DoC to administer the certification process. In the second year of operation of the Privacy Shield, the DoC has developed new procedures and further improved the certification process based on its experience in the first year and the Commission's recommendations. In addition, at the time of the review meeting, several companies had completed their first year of certification and had gone through the re-certification process. The second annual review therefore also looked at the functioning of the re-certification process.

At the date of the review meeting, 3,858 companies had certified under the Privacy Shield. In its first two years of operation, the Privacy Shield therefore has almost reached the same

[12] Namely, Cisco, Workday, Salesforce and Baker MacKenzie, a law firm that advises many Privacy Shield-certified companies.

number of certified companies as its predecessor, the Safe Harbor arrangement, had obtained after 13 years of existence (i.e. just over 4,000 participants).

Among those, more than 2,100 companies re-certified after their first year of participation in the framework (there is currently a 93% re-certification rate). The DoC noted that interest in the framework is increasing, with more than 1,200 first-time applications since April 2018. At the time of the second annual review, more than 1,000 applications for certification were still under review by the DoC.

During the second annual review meeting, the Commission services asked for further clarifications on the verifications carried out by the DoC during the certification process.[13] In particular, the Commission services inquired about the level of clarity and detail required by the DoC from companies when they describe their activities with respect to personal information received from the EU.[14] The DoC explained that it reviews the completion and consistency of the information in the certification form: it verifies whether this information is concise and understandable, and carries out cross-checks to ensure that what is indicated on the certification form matches the company's privacy policy. This is a crucial step to allow individuals to understand which activities of a Privacy Shield-certified company are covered by its certification and ultimately, whether or not they can rely on the safeguards afforded by the framework and invoke the rights it confers. When the DoC considers that the provided information is incoherent or insufficient (for example when there is an insufficient indication of the purpose of processing or a clear contradiction between what is in the certification form and the privacy policy) it will go back to the company to ask for further clarifications.

The Commission services also asked for additional explanations about the verifications carried out by the DoC when companies indicate that their Privacy Shield certification would cover several entities and subsidiaries.[15] It is crucial that all entities and subsidiaries that are covered by a Privacy Shield certification individually meet the certification requirements. Moreover, it should be clearly communicated which entities are covered by a Privacy Shield certification to allow individuals to determine whether they can rely on the protections of the framework. The DoC confirmed that, when several entities and subsidiaries of one company are included in an application, it verifies whether the privacy policies of each of those entities meet the certification requirements and are available online.

It results from the review that throughout 2018 the DoC has further developed and refined the certification process. Firstly, the DoC decided to focus its work on addressing issues that arose during the second year of operation of the framework. For example, as it emerged that

[13] In accordance with the framework, the DoC verifies whether companies that apply for certification meet all certification requirements, see Annex I (Annex 1) to the adequacy decision, p. 3 and Annex II to the adequacy decision, para. 2.

[14] As part of the certification process, the DoC requires a brief description of the purposes of personal data processing, which is published on the Privacy Shield website when the certification is completed.

[15] When applying for a Privacy Shield-certification, companies must indicate which of its entities or subsidiaries will adhere to the Privacy Shield Principles. In accordance with the Notice Principle (Principle 1), Privacy Shield-certified organisations also have to inform individuals of the entities and subsidiaries that are covered by the certification.

several companies listed non-U.S. based entities and subsidiaries as entities to be covered by their Privacy Shield certification, the DoC decided to specifically work with organisations on this issue and developed internal guidelines for its Privacy Shield team.[16]

Secondly, the DoC introduced new elements to the certification procedure. The DoC introduced a new check, in addition to the verifications required by the framework, by which it verifies whether companies' privacy policies contain a hyperlink to the correct complaint form on the website of the respective complaint handling body. This ensures that individuals can easily find their way not only to the correct complaint handling body, but also to the relevant form to use for their complaint.[17]

Thirdly, in response to the Commission's recommendation, the DoC improved the procedure for first-time certification applicants. During the first annual review meeting, it emerged that companies were publicly referring to their adherence to the Privacy Shield before their certification had been finalised by the DoC.[18] To avoid legal uncertainty and false claims, the Commission recommended that companies should not be allowed to make public representations about their Privacy Shield certification before the DoC has finalised the certification and included the company on the Privacy Shield list.

In January 2018, the DoC informed the Commission services that it had introduced this change requested by the Commission. During the second annual review meeting, the DoC explained that since February 2018 a new process has been adopted, by which the DoC first has to conclude that a company fulfils all certification requirements and has to notify the company accordingly, before the company may publicly refer to its adherence to the Privacy Shield framework. Once the privacy policy is public, the company notifies the DoC, which then includes the company on the Privacy Shield list without delay. This ensures that companies certifying for the first time are required to delay public representations regarding their Privacy Shield participation until their certification review is fully completed by the DoC. The Commission services welcome this improvement to the procedure.

The process for annual re-certification is similarto the certification procedure: when companies apply for re-certification, the DoC reviews the privacy policy for all Notice Principle elements, the ongoing registration with an Independent Recourse Mechanism ("IRM"), the payment of applicable fees and compliance with the Self-Certification Principle (Supplemental Principle 6). Once a company applies for re-certification, the procedure has to be finalised within 45 days. If this is not the case, the DoC requires the removal of all references to the company's participation in the framework and the company is moved to the Inactive List.

[16] The online guide to certification also specifies that an organisation should list its "U.S. based" covered entities, see http://www.privacyshield.gov/ps-online-submission-guide

[17] The annual report of one of the independent recourse mechanisms ("IRM") (BBB, see section 4.1.4.2) mentions that it sometimes receives complaints that concern a company that has designated another IRM as complaint handling body under the Privacy Shield.

[18] See section 4.1.1 of the Commission Staff Working Document section 4.1.1, page 8.

The information provided by the DoC on the re-certification process was confirmed by the replies to the Commission's questionnaire from trade associations and companies, who found the re-certification process comparable to the certification process in terms of thoroughness (involving follow-up questions and active involvement from the DoC). Although companies reported that the overall process is straightforward and efficient, one of the difficulties that was raised is that the DoC provides limited information, in particular on the requirements for re-certification, the status of re-certification, the length of the process and the DoC's response time for inquiries.

During the second annual review meeting, the DoC informed that it has undertaken steps to improve communication with companies. The DoC works with companies in order to put in place multiple points of contacts who receive updates about certification requirements. Initially, some companies designated only one contact point and the DoC explained that it had encountered difficulties where, due to staff turnover in companies, points of contact had changed or were no longer available and automatic reminders and updates were therefore not received.[19]

It also resulted from the second annual review that companies that are still in the process of re-certification after their initial certification has lapsed, continue to be listed on the Privacy Shield website and continue to refer to their adherence to the Privacy Shield Principles before the re-certification process has been completed by the DoC. The DoC explained that sometimes the re-certification process is initiated before the "end date" of the initial certification and continues after this date has lapsed. According to the DoC, in many cases this is due to confusion about formal requirements, such as the payment of fees, which require a back and forth between the DoC and the company. The DoC also provided reassurance that, even if there is this time gap because the re-certification process is not finalised, there is no lapse in protection, since the commitments of the company remain fully enforceable. Moreover, this time gap would last for a maximum of 45 days, which is the time frame in which the re-certification must be finalised.[20]

At the time of the second annual review meeting, the DoC was in the process of making technical changes to the certification process to ensure that a company's next certification due date would be 12 months from the date it has submitted its annual re-certification (instead of 12 months from the date the re-certification is finalised).[21] When a company's certification lapses and the company is not in the process of re-certifying, a Failure to Re-

[19] For example, in response to the Commission's questionnaire addressed to trade associations, one company reported that it had not received reminders when its certification was about to lapse. The DoC explained during the first annual review and confirmed during the second annual review that automatic reminders are sent one month prior to the anniversary of the initial certification data and again two weeks and then one day prior to that day.

[20] If the re-certification is not finalised within 45 days, the company is required to remove all references to its participation in the Privacy Shield and is removed to the Inactive List. In this case, the company can therefore no longer rely on the Privacy Shield to receive personal data from the EU.

[21] The Privacy Shield website displays the original certification date of each certified company, as well as the date of the last certification and the due date for the upcoming re-certification.

certify Questionnaire is issued and the company is automatically moved to the Inactive List on the Privacy Shield website.

At the date of the second annual review meeting, around 360 companies were on the Inactive List on the Privacy Shield website. According to the DoC, those companies 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.[22] When a company withdraws voluntarily, it is required by the DoC to complete a Withdrawal Questionnaire. The withdrawing company has to indicate whether it intends to retain the personal data received under the Privacy Shield and if yes, what safeguards it will continue to apply. By 1 August 2018, 38 companies had withdrawn from the Privacy Shield framework. 17 of those chose to return or delete the personal data they collected under the Privacy Shield, 9 chose to retain the data and provide "adequate protection""[23], while 12 chose to retain the data and continue to apply the Privacy Shield Principles.

The Commission services note that the certification process has been further strengthened, including by the implementation of the recommendation from the first annual review. At the same time, the Commission services stress the importance of continuous monitoring of the functioning of the (re-)certification process and introducing improvements as new questions emerge.

4.1.2. Monitoring and supervision by the Department of Commerce

In the Commission Staff Working Document on the first annual review, the Commission services noted that the DoC's efforts during the first year of operation of the Privacy Shield focused more on certification than on monitoring and supervision.[24] In particular, although the DoC had developed instruments to ensure supervision of compliance by certified companies with the Privacy Shield Principles, e.g. Compliance Review Questionnaires, these tools had not yet been used. The Commission highlighted that the DoC should make use of the tools it has developed and recommended to the DoC to conduct compliance checks on a regular basis.

In January 2018 the DoC informed the Commission services that it had implemented a new mechanism of "spot checks", by which it 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 IRM is available to handle

[22] According to the information provided by trade associations and companies, some reasons not to (re)-certify include corporate or business changes, changes to activities where personal data from the EU is no longer collected and the use of other transfer tools (in particular Standard Contractual Clauses and Binding Corporate Rules). Concerns about onerous requirements (in particular the Onward Transfer Principle), as well as the validity and long-term stability of the Privacy Shield were also raised as reasons not to apply for certification or re-certification.

[23] See Supplemental Principle 6(f).

[24] See section 4.1.2 of the Commission Staff Working Document.

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.[25] If there is no timely and satisfactory response, the DoC sends a warning letter requiring the company to indicate within 30 days how it has addressed the detected issue(s). If the issue(s) would not be resolved by the end of that 30-day period, the organisation would be removed from the Privacy Shield list and placed on the Inactive List.

The current focus of the spot-checks is the availability of recourse mechanisms for individuals, in particular by verifying whether points of contact are responsive and companies have registered with an IRM. As the use of this mechanism further develops, other elements could be included in the spot-checks. During the second annual review meeting, the DoC informed that it had already performed spot-checks on 100 organisations and will continue this practice in the future. In 21 cases, relevant compliance issues were detected and a Compliance Questionnaire was issued. These issues concerned the lack of response from a designated point of contact, privacy policies that were no longer accessible online and missing references to one or more elements of the Notice Principle. All 21 companies responded to the Questionnaire and rectified the detected issues.

Aside from the spot-checks, the DoC has also developed three additional compliance review procedures since the first annual review. Firstly, a member of the DoC Privacy Shield team is now 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 or reasonable belief that compliance with the Privacy Shield Principles could be affected, it initiates the compliance process by sending the Compliance Questionnaire. During the second annual review meeting, the DoC informed that it had looked at five incidents that were detected through this mechanism.This is important to link a company's compliance with its specific obligations under Privacy Shield with the broader context in which it operates.

Secondly, the DoC conducts "sweeps" of Privacy Shield participants' websites to identify broken links to privacy policies. At the time of the second annual review, only one broken link had been detected. The DoC informed that it plans to perform such sweeps regularly in the future.

Finally, the DoC engages with Privacy Shield-certified companies to ensure that the information provided on the Privacy Shield website remains up to date. When companies indicate certain changes, e.g. changes in contact information, change in organisation name, change in type of data that is covered (HR data/non-HR data), the DoC works with them to update the available information.

Another channel through which the DoC detects potential compliance issues is through referrals from EU data protection authorities ("DPAs"). In one instance, the DoC served as a liaison between an EU DPA and a Privacy Shield-certified company after receiving an informal referral from the DPA which indicated that the details of a company's point of

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

contact were not available. No formal referral process had however been triggered yet at the time of the second annual review.[26]

The Commission services note that the DoC has stepped up the monitoring of compliance in the second year of operation of the Privacy Shield. In line with the Commission's recommendation, the DoC has made use of several tools to proactively monitor compliance with the Privacy Shield Principles and has introduced new mechanisms to detect potential compliance issues. At the same time, the Commission services consider that, in the absence of complaints (see below, section 4.1.4) or referrals by DPAs, it is at this stage not possible to fully assess the effectiveness of these procedures, which will have to be closely monitored in the context of future annual reviews.

In its Staff Working Document on the first annual review, the Commission services had also addressed the oversight role of the DoC with respect to false claims of participation in the Privacy Shield framework. In particular, the Commission services noted that the DoC had not yet conducted active searches for false claims.[27] The Commission therefore recommended that the DoC conducts, proactively and on a regular basis, searches for false claims of participation in the Privacy Shield, not only in the context of the certification process, but also more generally with respect to companies that have never applied for certification but make representations suggesting to the public that they comply with the framework's requirements.

In January 2018, the DoC informed the Commission services that, in order to identify false claims, it developed a prioritisation plan and a system for image and text searches on the internet. During the second annual review meeting, the DoC further specified the way it conducts false claims reviews. On a quarterly basis, the DoC targets 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.

In addition, the DoC looks more generally for false claims through text searches on the internet using formulations commonly used by companies to refer to their participation in the Privacy Shield. According to the DoC, some non-certified companies could have copied it to falsely claim their participation in the framework. Moreover, a Privacy Shield logo is currently being developed and once finalised, image searches will look for that logo on companies' websites. During the second annual review meeting, the DoC explained that there is no specific time frame to conduct internet searches, but they will continue to take place in the future. So far, most issues that were identified through internet searches had been already detected by the DoC through other processes.

A third way by which the DoC conducts false claims reviews is in response to information received from DPAs, IRMs, businesses and individuals. So far, the DoC has received such information in no more than a handful of instances (e.g. one false claim referral from an individual).

[26] See section 4.1.3.3 of the Commission Staff Working Document, p. 16.
[27] See section 4.1.2 of the Commission Staff Working Document, p. 11.

If the DoC detects issues indicating potential non-compliance with the Privacy Shield Principles or false claims of participation in the framework, it sends a certified letter warning the identified companies of a potential referral to the FTC/DoT if outstanding requirements are not fulfilled or participation references are not removed. The FTC/DoT are informed of the DoC's intention to send such letters. If a company fails to respond to the letter within 30 days, it is included in a referral list compiled by the DoC that contains the organisations that failed to respond to take action within the defined timeframe. Since the launch of the program, the DoC has sent over 400 warning letters. Most concerns were resolved within the 30-day timeframe.

Since the first annual review, the DoC has referred 56 companies to the FTC (since the start of the Privacy Shield program, more than 100 companies have been referred). These referrals concern both issues of non-compliance and false claims. The main detected non-compliance issues that led to an FTC referral concerned non-compliance with the Notice Principle and lack of information provided in the privacy policy on recourse mechanisms. In most cases, the referral itself was sufficient to ensure that the concerned company took the necessary action to resolve the identified issue (see also section 4.1.3).

When a company is referred to the FTC it is moved to the Inactive List.[28] The DoC continues to cooperate with the relevant company after the FTC referral to address the underlying concerns. During the second annual review meeting, the DoC explained that, in many instances, the referral concerns the payment of fees, rather than substantive issues. Companies can still resolve the detected issue after the referral, for example by responding to the Withdrawal Questionnaire after a certification has lapsed. The DoC has an "FTC liaison" that cooperates with the FTC by providing relevant information on referrals, such as copies of relevant correspondence with a company, and by providing updates on any action taken by the referred company since the referral took place.

The Commission services welcome that, also in the search for false claims, the DoC has developed new procedures and is actively using different tools, in accordance with the Commission's recommendation. The Commission services furthermore note that the DoC's efforts, both on detecting compliance issues and false claims of participation, have led to a number of referrals to the FTC. At the same time, as the different tools introduced by the DoC in both areas are still in their initial stages of use, further monitoring to determine their effectiveness will be important. Against this background, the third annual review will have to assess in particular the effectiveness of the tools used to identify false claims by organisations that have never applied for certification and issues of compliance with susbstantive obligations.

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

[28] As a result, it can no longer publicly refer to its participation in the Privacy Shield and can no longer rely on the framework to receive personal data from the EU.

Since the first annual review there have been important developments concerning the FTC that are relevant for the functioning of the Privacy Shield.

As regards the structure of the FTC, in May 2018, a new Chairman and three new Commissioners were sworn in, ensuring that the FTC had all five Commissioners in place. The Commission services note that, even though the FTC continued to be fully functioning also prior to May 2018, the situation has significantly improved compared to last year when there were only two Commissioners.

Concerning the enforcement of the Privacy Shield, several actions have been taken by the FTC in the second year of operation of the framework. Of the 56 referrals from the DoC to the FTC, five have led to enforcement action by the FTC (see section 4.1.2. During the two years of operation, there have been over 100 referrals in total, eight of which led to enforcement). Some referrals are still under investigation, while in other cases the relevant companies came into compliance before the FTC initiated enforcement. There were no referrals to the FTC from the EU DPAs in the second year of the Privacy Shield.

More specificallly, on 2 July 2018, the FTC reached a settlement (a so-called "consent agreement" or "consent order") with a company regarding charges that it had falsely claimed being certified under the Privacy Shield.[29] On 27 September 2018, the FTC announced that it had reached a settlement with four more companies who falsely claimed participation in the Privacy Shield (one had never completed its certification with the DoC[30] and three had let their certification lapse[31]). The FTC further alleged that two companies had also failed to abide by the Privacy Shield requirement that companies that stop participation affirm to the DoC that they will continue to apply the Privacy Principles to personal data collected while participating in the program.[32] This brings the total number of cases brought by the FTC to enforce the Privacy Shield framework to eight.[33] At the time of the second annual review, only four of these eight cases were final, while the remaining four were still open to public comments. Consent orders are placed on the record for public comment during a period lasting for 30 days before they can become final.

With respect to the follow-up to those consent orders that have become final, the FTC explained that final consent orders are included in the FTC's enforcement database and sent to a dedicated FTC department. Each consent order has a designated compliance attorney who is responsible for monitoring compliance with the order, for example by obtaining compliance reports or searching for online information on the concerned company. At the

[29] See the decision and order of the FTC in the matter of ReadyTech Corporation of 2 July 2018.
[30] See the decision and order of the FTC in the matter of IDmission of 27 September 2018.
[31] See the decisions and orders of the FTC in the matters of mResource, SmartStart Employment Screening and VenPath of 27 September 2018.
[32] See the decisions and orders of the FTC in the matters of Venpath and SmartStart Employment Screening of 27 September 2018.
[33] See 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), p. 17 and the consent agreements in the matters of Decusoft, Tru Communication and Md7, announced by the FTC on 8 September 2017.

time of the second annual review, this process was ongoing for the four final consent orders relating to the Privacy Shield and there had been no occasion for the FTC to take further action.[34] In the context of the implementaion of the consert orders, the Commission services will monitor in the coming years whether, pursuant to Principle 7(e), companies subject to an FTC order make public any relevant Privacy Shield-related sections of compliance or assessment reports submitted to the FTC.[35]

The Commission services welcome the enforcement action taken by the FTC regarding cases of false claims since the first annual review. At the same time, the Commission services had also expressed the expectation in the Staff Working Document on the first annual review that the FTC will not only investigate false claims, but also Privacy Shield compliance issues.[36] The Commission services underlined the importance of developing a more strategic and proactive approach to enforcement, for example by looking "thematically" at how companies comply with the Privacy Shield, e.g. by means of "sweep actions". The importance of such an approach has become even more apparent in light of recent revelations about large-scale data misuse and breaches.

During the second annual review meeting, the FTC informed that it had taken action in response to the Commission's recommendations.[37] In particular, it has started carrying out ex officio sweeps by sending out administrative subpoenas to check for substantive violations of the Privacy Shield. Administrative subpoenas are a general (court enforceable) tool at the FTC's disposal to obtain information as part of a law enforcement investigation. They are regularly used by the FTC in consumer protection and privacy cases, and are now also deployed in the context of potential Privacy Shield compliance issues.

Although the FTC was not in a position to provide detailed information on the administrative subpoenas that have been issued with respect to Privacy Shield-certified companies, it was explained during the second annual review meeting that the FTC has various ways to decide how to focus its work, for example on a particular industry or compliance with a specific Privacy Principle. The scope of such type of investigation can be broad since a reasonable suspicion of non-compliance is not a prerequisite to send a subpoena. The Commission services welcome that the FTC is developing a more pro-active approach to the enforcement of the Privacy Shield Principles by applying its practice of sending administrative subpoenas in a Privacy Shield context. While it is clear that the use of sweeps raises, like any official investigation, issues of confidentiality, it is very regrettable that the FTC provided only limited information at the annual review meeting.

[34] The FTC has the power to enforce final consent orders by bringing violations of a consent order to court, in order to obtain consumer redress, civil penalties, injunctions or other equitable relief, see also the explanations provided at the FTC's website: https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.
[35] See also Annex IV to the adequacy decision, section IV.
[36] See section 4.1.4 of the Commission Staff Working Document, p. 17.
[37] See also the remarks by FTC Chairman Simons:
https://www.ftc.gov/system/files/documents/public_statements/1416593/chairman_joe_simons_privacy_shield_review_remarks-2018.pdf

The fact that the FTC announced commitment to a more proactive approach in this area is a promising development. Further steps taken in these investigations, including as regards their outcome, will be very closely monitored and will represent a central point of the third annual review as well as future ones. This will allow an assessment of the effectiveness of the Privacy Shield's enforcement mechanisms. This is also why the FTC should find ways to share information, including with EU DPAs that also have responsibilities in the enforcement of the Privacy Shield, on such a crucial aspect of the overall functionning of the framework.

The FTC also confirmed that it continues to systematically look for potential Privacy Shield violations as part of its privacy and security investigations.[38] When opening an investigation, the FTC always checks whether the concerned company is Privacy Shield-certified. As an example, the FTC explained that when investigating a case concerning an alleged data breach, it would verify whether the concerned company is a Privacy Shield participant and if this would be the case, would examine whether the company put in place procedures that comply with the Security Principle (Privacy Shield Principle 4).

As part of its privacy and security investigations, the FTC was at the time of the second annual review investigating the Facebook/Cambridge Analytica case. In March 2018 a whistle-blower (a former employee of Cambridge Analytica) revealed that Cambridge Analytica had harvested the personal data of millions of individuals' Facebook profiles without their consent. At present, Cambridge Analytica and its parent company (SCL Elections LTD) are no longer on the Privacy Shield list because their certification lapsed in June 2018.

On 26 March 2018, the FTC issued a statement in which it confirmed that its investigation into Facebook's privacy practices would also cover potential violations of the Privacy Shield. At the time of the second annual review, the FTC was not in a position to share information on the case as the investigation was still ongoing. The Commission services welcome that the FTC is also looking into potential Privacy Shield violations in its ongoing investigation of Facebook and look forward to receiving more information once the investigation is finalised. Once again, these are issues of common interest to enforcers on both sides of the Atlantic and more information should be shared by the FTC, including in a confidential way where necessary. During the second annual review meeting, the DoC also confirmed that Facebook will be removed from the Privacy Shield list should the FTC determine it failed to comply with its commitments under the framework.

With respect to more general developments, the Commission services note that, in its new composition, the FTC has initiated a process of reflection on its current power in the area of privacy. On 20 June 2018, the FTC announced that it would hold a series of public hearings that will, among other topics, deal with the FTC's remedial authority to deter unfair and deceptive practices in privacy and data security matters. The process also looks into the efficacy of the FTC's use of its current remedial authority and the identification of any additional tools or authorities the FTC may need to adequately deter unfair and deceptive

[38] See also Annex IV to the adequacy decision.

conduct related to privacy and data security. During the second annual review meeting, the FTC confirmed that it is seeking public comments on how it can make use of its existing powers in the most effective way. The Commission services note the FTC's initiative with interest and consider that further enhancing the enforcement mechanism in the area of privacy would reinforce the foundations of the Privacy Shield.

Finally, the FTC informed about two case law developments in 2018 with relevance for the Privacy Shield.

First, in the case of *FTC v. AT&T* (decision of the U.S. Court of Appeals for the Ninth Circuit of 26 February 2018) it was confirmed that the FTC has jurisdiction over non-common carrier activities of companies qualifying as common carriers (which are regulated by the Federal Communications Commission (FCC)). The case therefore confirms that common carriers can certify under the Privacy Shield for non-common carrier services.

Second, in the case of *LabMD v. FTC* (decision of the U.S. Court of Appeals for the Eleventh Circuit of 6 June 2018), the Court of Appeals found that an FTC cease and desist order against LabMD was unenforceable because it was too vague (the order did not point to a specific act or practice of LabMD and did not specify how the ordered overhaul of LabMD's data security program should be accomplished). During the second annual review meeting, the FTC confirmed that this case concerns one specific FTC order and does not affect the FTC's authority under Section V of the FTC Act to enforce privacy and data security issues.

4.1.4. Complaint handling

During the first annual review meeting, it emerged that a number of tools and mechanisms were put in place in the first year of operation of the Privacy Shield framework to ensure an effective handling of complaints.[39] As the number of complaints received by the various redress mechanisms[40] was very low during the first year, the Commission concluded that the handling of complaints will be assessed more in depth in future annual reviews.[41]

4.1.4.1. Complaint handling by companies

Based on the information provided by trade associations and companies, it appears that, also in the second year of the Privacy Shield, very few complaints were lodged with Privacy Shield companies: it results from the answers to the questionnaire that only one respondent company received "a few" complaints.

On the other hand, several companies reported that they have received a certain number of general inquiries about the Privacy Shield, in particular concerning companies' certification

[39] See section 4.1.3 of the Commission Staff Working Document.
[40] The Privacy Shield provides several alternative redress possibilities: individuals can bring a complaint i) directly to a Privacy Shield-certified company, ii) to a free-of-charge independent recourse mechanism ("IRM"), iii) to an EU DPA or iv) directly to the FTC. Moreover, v) as a 'last resort' mechanism, an individual can have recourse to an arbitration mechanism: the Privacy Shield Panel.
[41] See section 4.1.3 of the Commission Staff Working Document, p. 13.

status, whether the certification covers all their products and how their Privacy Shield certification relates to the GDPR. In addition, companies received questions on privacy in general, e.g. concerning compliance with the GDPR. Privacy Shield inquiry forms are sometimes also used by individuals to seek general account/product-specific support.

Companies also reported to have received requests for access to data, requests to opt-out from data sharing with third parties and requests for information (e.g. on deletion and data retention policies). To enable individuals to exercise their rights and deal with requests, Privacy Shield certified companies have put in place technical tools and mechanisms, such as dedicated e-mail addresses, online mechanisms and webforms. At the same time, companies sometimes also receive requests through mechanisms that are not specifically dedicated to the Privacy Shield, for instance traditional customer support processes.

It therefore seems that, although data subjects are making use of the possibility to exercise their rights, the number of formal complaints remains low. Together with the information provided by IRMs in their annual reports (see section 4.1.4.2.), this seems to indicate that data subject requests are generally resolved without further escalating to formal complaint procedures or other dispute resolution mechanisms.

4.1.4.2. Complaint handling by independent recourse mechanisms (IRMs)

In accordance with recital 45 of the adequacy decision and Supplemental Principle 11(d)(iii) (Dispute Resolution and Enforcement), all IRMs are required to publish an annual report providing aggregate statistics regarding their services. Reports for the period 1 August 2017-31 July 2018 had been issued by the time of the second annual review. Although the number of complaints received by IRMs in the second year of operation of the Privacy Shield is higher compared to the first year,[42] the large majority of complaints were ineligible, as they did not concern data that had been transferred under the Privacy Shield, and the overall number of complaints remains low. In total, IRMs received 38 eligible complaints, all of which were resolved in a timely manner. The majority of complaints were related to requests to change or remove personal data, to unsubscribe, to address disabled accounts and to connect with a company representative. The EU DPA Panel[43] did not receive any complaints.

More specifically, Better Business Bureau (BBB) received 525 complaints (compared to 180 complaints the previous year), with 101 originating from the EU and Switzerland. However, none of the complaints was ultimately found eligible. The majority of complaints was directed either at companies that had not chosen BBB as IRM or were not Privacy Shield certified. Of the remaining complaints, only two were related to privacy and were dropped by the complainant following requests for additional information. When BBB receives complaints addressed to companies that have chosen a different IRM, it directs the concerned individual to the Privacy Shield website where the correct IRM is indicated.

[42] See section 4.1.3.2 of the Commission Staff Working Document.
[43] Recitals 48-51 of the adequacy decision.

As another example, TrustArc received 301 complaints from EU individuals, of which only 30 were eligible Privacy Shield-related complaints. At the close of the annual report, 10 additional complaints were pending a determination of eligibility. The majority of complaints concerned account hacking/disabling/suspension (6), changes to/deletion of personal data (9) and difficulties with unsubscribing (6).[44] In 12 cases, personal data was removed, accounts were closed or credentials were validated. In 3 cases, changes were required to the website or practices of the company. In the remaining cases, either no changes were required (9), or the individual unsubscribed (6). Approximately 22 percent of the total number of complaints from EU and Swiss individuals (309) were closed on procedural grounds, e.g. complaints that fail to state a comprehensible issue. Similar information is reported by other IRMs: the majority of complaints turn out to be ineligible, because they contain an incoherent message, do not come from EU individuals, or are not related to the Privacy Shield.[45]

The Commission services note that the terminology used by IRMs varies across the different annual reports. While some reports refer to "complaints from EU individuals" others refer to "complaints originating from Europe". During the second annual review meeting, it was clarified that the IRMs handle complaints from EU data subjects within the meaning of the Privacy Shield, i.e. individuals whose personal data has been transferred from the EU to Privacy Shield-certified companies regardless of nationality or residence.[46] As was also mentioned in the Staff Working Document on the first annual review, the annual reporting by IRMs should be harmonised to allow a clear comparative reading, including in terms of terminology.[47]

Finally, it follows from the annual reports that IRMs often also offer external compliance review services. This was confirmed by the replies to the questionnaire addressed to trade associations: several respondent companies[48] indicated that they have indeed chosen the same provider for dispute resolution services and external compliance review.[49] During the second annual review meeting, the DoC explained that potential conflicts of interest related to these two functions are prevented by establishing separate chains of command and separating the

[44] Other types of complaints: account access/creation (2), children's information (1), help with features/functionality (1), inaccurate privacy disclosure (1), difficulties with contacting participating sites (3), and unauthorized profile with personal information (1).

[45] Privacy Dispute Resolution Services (PDRS), Whistic and International Centre for Dispute Resolution (ICDR) received no Privacy Shield-related complaints during the reporting period. VeraSafe reported not to have received eligible complaints. JAMS received two eligible claims, both of which were resolved within one month (without specifying what the claims were about). PrivacyTrust received 14 complaints, all of which were ineligible (there was no coherent message or the complaint was unrelated to the Privacy Shield). DMA received five eligible complaints which were resolved within 1 to 9 days. Eight inquiries were found ineligible because they originated from the U.S. or did not contain a clear message. The eligible complaints concerned e-mail removal, a request to remove an online picture and a request from the Spanish Intellectual Property Commission regarding registering its online advertising services.

[46] See recitals 16 and 17 of the adequacy decision.

[47] Commission Staff Working Document section 4.1.3.2, p.15.

[48] 48 respondent companies reported to use the same provider for dispute resolution and external compliance review.

[49] Supplemental Principle No. 7 of the Privacy Shield principles (Annex II to the adequacy decision) requires Privacy Shield companies to provide follow-up procedures for verifying that their assertions about their Privacy Shield practices are true and those practices have been implemented in accordance with the Privacy Shield Principles. Companies can choose to do this either through self-assessment or outside compliance reviews.

duties of employees. As an example, it was mentioned that TrustArc specifically addresses this issue by having separate teams dealing with dispute resolution on one hand and compliance on the other. The DoC announced that the annual reports of the IRMs in the third year of operation of the Privacy Shield framework will specifically address the mechanisms that have been put in place to avoid any conflict of interest.

4.1.4.3. Complaint handling by the DoC, FTC and DoT

Also in the second year of operation of the Privacy Shield framework, the DoC did not receive any complaints from individuals. The FTC received six Privacy Shield-related complaints (four concerning false claims), one of which was being investigated at the time of the second annual review. Four concerned companies that were not Privacy Shield-certified and one concerned a non-profit organisation that was not eligible to participate in the framework.

The DoT has not received any complaints on the Privacy Shield, and very little privacy related complaints in general. This follows also from the fact that there are currently no airlines and a very low number of ticket agents participating in the Privacy Shield. During the second annual review meeting, the DoT informed that, if it would receive a Privacy Shield-related complaint, it would coordinate with the DoC and FTC.

4.1.4.4. The Binding Arbitration Mechanism

As of January 2018, the arbitration panel has been fully operational. All arbitrators have been selected and, at the time of the second annual review, a pool of 22 arbitrators had been established.[50] The arbitrators who were selected by the DoC and the Commission come from a variety of professional backgrounds, including legal practitioners with arbitration expertise, a former member of the judiciary, law professors from highly reputed academic institutions, etc. They also represent different legal traditions, with arbitrators coming from the U.S., EU Member States as well as other third countries, and have demonstrated experience in U.S. privacy and EU data protection law.

Moreover, as secretariat, Arbitral Administrator and Fund Manager of the Binding Arbitration Mechanism, the International Centre for Dispute Resolution of the American Arbitration Association (ICDR-AAA) has put in place Binding Arbitration Rules and a Code of Conduct. ICDR-AAA has made all relevant information available on its website and reports weekly to the DoC on the status of the Arbitral Fund. The ICDR-AAA website provides clear and concise information to companies on the Arbitral Fund, as well as to individuals about the arbitration mechanism and the procedure to file for arbitration.[51] The Commission services welcome that the Arbitration Panel is now fully operational.

[50] The Privacy Shield requires a pool of at least 20 arbitrators; see Annex 2 to ANNEX I of the adequacy decision.
[51] See https://www.icdr.org/privacyshield.

At the time of the second annual review, the Binding Arbitration Mechanism had not been triggered.

4.1.5. Automated individual decision-making

In its Staff Working Document on the first annual review, the Commission concluded that further information was needed on the issue of automated decision-making and committed to commission a study to collect factual evidence and further assess the relevance of automated decision-making for transfers carried out on the basis of the Privacy Shield.[52]

The Commission therefore commissioned a study to determine:

(i) the extent to which Privacy Shield-certified companies in the U.S. take decisions affecting individuals based on automated processing of personal data transferred from companies in the EU under the Privacy Shield; and

(ii) the safeguards for individuals that U.S. federal law provides for this kind of situations and the conditions for these safeguards to apply.[53]

The study consists of two parts: an evidence-based analysis and an analysis of the relevant U.S. legal framework. The evidence-based analysis relies on different sources: annual reports published by IRMs, interviews with legal and technical experts, and two case studies focussing on the supply of the two main elements for automated decision-making: data and (analytics and decision-making) software.

On the first aspect, the study concludes that automated decision-making is still an emerging technology and there is currently no evidence suggesting that automated decision-making is normally being carried out by Privacy Shield-certified companies on the basis of personal data transferred under the Privacy Shield. At the same time, since it is an area that is rapidly evolving, it should be closely monitored. The study identifies several areas in which the use of automated decision-making is overall most likely to take place. These areas are financial (e.g. credit scoring, commercial loans, commercial insurance) and human resources, with health as an emerging sector.

The legal analysis concludes that, although there is no overarching federal legislation in the U.S. that would apply to automated decision-making, several sectoral laws apply in the identified areas and provide for specific safeguards that are similar to those of the GDPR. In the area of consumer credit, the Fair Credit Reporting Act (FCRA) and Equal Credit Opportunity Act (ECOA) contain safeguards that provide consumers with some form of a right to explanation and a right to contest the decision. These Acts are relevant in a wide range of areas, including credit, employment, housing and insurance, where it is most likely that companies would resort to automated processing.

[52] See section 4.1.5 of the Commission Staff Working Document.
[53] The study has been published on the Commission's website (https://ec.europa.eu/info/law/law-topic/data-protection_en)

In addition, certain anti-discrimination laws, such as Title VII of the Civil Rights Act and the Fair Housing Act provide individuals with protections with respect to models used in automated decision-making that might discriminate on the basis of certain characteristics and provide individuals with rights to challenge decisions, including automated ones.

With respect to health information, the study concludes that the Health Insurance Portability and Accountability (HIPAA) Privacy Rule creates certain rights that are analogous to those of the GDPR with respect to accessing personal health information. In addition, guidance from the U.S. authorities require medical providers to receive information that allow them to inform individuals of automated decision-making systems used in the medical sector.

Finally, Section 5 of the Federal Trade Commission Act prohibits unfair or deceptive acts or practices, which according to the study "*serves as a broad check on decisions based on automated processing that may be unfair or deceptive*".

At the second annual review meeting, the FTC presented a recent case in which it had enforced the Fair Credit Reporting Act to a situation of automated decision-making. The case was brought against RealPage, Inc., a tenant screening company which offers a criminal background screening system used by landlords to check consumers who are trying to lease an apartment. The FTC alleged that RealPage, Inc. did not take reasonable measures to ensure the accuracy of the information that it provided to landlords on the basis of its auto-decision tool which sifts through all court records. The company agreed to settle the charges against a fine of 3 million USD.[54] This case appears to confirm that the protections of the Fair Credit Reporting Act are not narrow, but apply to any significant decision that is made on the basis of consumer data, including in the area of housing, employment and insurance.

The replies received in response to the questionnaire addressed to trade associations seem to confirm the findings of the study. Only eight respondent companies reported to use personal data that has been transferred from the EU to the U.S. on the basis of the Privacy Shield for automated decision-making, without specifying in which area this takes place. One company reports that it does not act as the decision-maker, but provides analytical capabilities to its customers that empower these to make decisions. This is also confirmed in the study, which notes that most providers of automated decision-making products, services and platforms would qualify as data processors and are not consumer-facing.

On the basis of the study and information received from Privacy Shield-certified companies, the Commission services conclude that, at present, there is little evidence that Privacy Shield-certified companies are engaging in automated decision-making on the basis of personal data transferred under the Privacy Shield. At the same time, it is the understanding of the Commission services that situations in which decisions based on automated processing are taken by companies in the U.S. are generally falling within the scope of the GDPR and its specific provisions in automated decision-making, as they typically involve companies that

[54] See https://www.ftc.gov/news-events/press-releases/2018/10/texas-company-will-pay-3-million-settle-ftc-charges-it-failed

are either present in the EU or have a direct relationship with EU customers.[55] This would also include scenarios where the processing is carried out by a Privacy Shield organisation acting as an agent on behalf of EU controllers.

However, since automated decision-making is a rapidly evolving area, it continues to require close monitoring in the context of future reviews.

4.1.6. Human resources data

At the first annual review, it 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 processing of data of employees of a Privacy Shield-certified company falls within the category of HR data under the Privacy Shield. The DPAs instead were of the opinion that 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 answers to the Commission's questionnaire addressed to trade associations indicate that, while many of the respondents do not use the Privacy Shield as a transfer mechanism for HR data, those that do so consider only the processing of personal data relating to their own employees for employment related purposes, as well as for purposes not directly related to their employment, to constitute processing of HR data. Several respondents indicate to also consider the processing of data of job applicants as HR data. At the same time, several respondents pointed out that they treat their customer's data as confidential and would therefore not even be aware of whether it contains HR data or not. It was also highlighted that if Privacy Shield-certified service providers in the U.S. were to use the data of their customers for different purposes than those agreed in the relevant contracts (i.e. for their own purposes), this would significantly affect their commercial relationship and might even lead to the termination thereof.[58] This was also confirmed during the presentations given by industry representatives at the second annual review meeting.

The notion of human resources data was mentioned by the Commission in its report on the first annual review as a concept that would benefit from additional clarification. The Commission services note that, since the first annual review, the DoC, the FTC and the DPAs have not been able to come to a common understanding regarding the notion of human resources data.

However, during 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 note that they made

[55] See Article 3(2) of the GDPR.
[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.
[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] For example, one respondent mentioned that it would bring them "*out of business*."

progress in understanding each other's position and agreed to continue their dialogue on this topic, with a view to identifying practical solutions to reconcile the terminology of the framework and to ensure that the necessary safeguards, in particularly the Choice Principle, are correctly applied to data that is collected in the EU in the context of an employment relationship and subsequently transferred to the U.S. under the Privacy Shield. The Commission services thus urge the EU and U.S. enforcers to continue their constructiuve dialogue with a view to issue common guidance on this important topic. Such guidance could give a valuable contribution to ensuring both legal certainty and a consistent level of protection.

4.1.7. Awareness-raising and cooperation between authorities

In its report on the first annual review, the Commission recommended that the DoC and the DPAs continue and further strengthen awareness-raising efforts. Since the first review, the DoC has complemented existing information on its website (with specific material tailored to U.S. businesses, EU businesses, EU individuals and DPAs) with a user-friendly factsheet informing EU and Swiss individuals about the Privacy Shield and the rights and recourse mechanisms that are available under the framework.[59] In addition, the DoC has worked on guidance addressed to Privacy Shield participants: answers to frequently asked questions have been updated and provide information on the Privacy Shield as a transfer tool under the GDPR, the requirements to certify, the annual fees, the information to include in privacy policies, requirements with regard to onward transfers, obligations for processors, etc.[60] Furthermore, there are new step-by-step instructions for completing the online certification application and explanations of procedures for both first-time applicants and re-certification.[61]

During the second annual review meeting, the DoC also confirmed that U.S. senior officials have participated in numerous events in the EU and the U.S. to raise awareness and to better explain the administration of the framework to the various stakeholders.

Since the first annual review, the DPAs have also engaged in different awareness-raising activities. During the second annual review meeting, the DPAs explained that they inform the general public by providing information on the Privacy Shield and the certification process on their websites, including by providing links to guidance on the Privacy Shield that is available on the Commission's website. Complaint forms for individuals (both for non-compliance with the Privacy Shield Principles and the Ombudsperson mechanism) are available on the websites of the DPAs, both in the official language(s) of the relevant Member State and in English. In addition, members of DPAs regularly participate in public events (conferences, seminars, etc.).

[59] See https://www.privacyshield.gov/Individuals-in-Europe
[60] See https://www.privacyshield.gov/article?id=FAQs
[61] See https://www.privacyshield.gov/article?id=How-to-Join-Privacy-Shield-part-1 and https://www.privacyshield.gov/article?id=How-to-Re-certify-to-Privacy-Shield

The Commission also recommended after the first annual review that the DoC and the DPAs should cooperate, if appropriate also with the FTC, to develop guidance on the interpretation of certain concepts in the Privacy Shield that need further clarification. Since the first review, the DoC worked together with the DPAs to develop guidance on the Accountability for Onward Transfer Principle and the application of certain Privacy Shield Principles in the controller-processor relationships. This guidance has been available on the Privacy Shield website in a question-and-answer format as of August 2018. In their replies to the Commission's questionnaire, several companies pointed out that this additional guidance has been helpful.

The Commission services welcome the cooperation of the DoC and the DPAs in developing additional guidance on certain principles of the Privacy Shield framework, in line with its recommendation, and encourage the DoC, the DPAs and, if appropriate also the FTC, to continue their cooperation and exchange on all questions related to the practical implementation of the framework, including the question of HR data (see also section 4.1.7).

At the same time, the Commission services note that, during the second year of operation of the Privacy Shield, new questions have emerged that require further clarification. In particular, from the information provided by trade associations and companies, there seems to be confusion among companies about the different tools for international transfers that are available under the GDPR. Some companies have pointed out that there is a need for guidance addressing the differences between the Privacy Shield and other data transfer tools.

The Commission services therefore encourage the DoC, the DPAs and where appropriate also the FTC to continue cooperating on the development of further guidance and to also monitor the need for additional clarifications.

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

In the second year of operation of the Privacy Shield, important developments took place with respect to the privacy legal framework in the U.S., which is currently characterised by a number of federal sectoral laws and numerous laws at state level. Legislative activity continued at state level, for example with the adoption of the California Consumer Privacy Act in June 2018. At the same time, there have been calls for action at federal level, in particular in light of recent 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, notably the revelations concerning Facebook/Cambridge Analytica and the data breaches at Equifax, Uber, Facebook etc. Against this background, the DoC has launched in June 2018 a dialogue with stakeholders on the development of a federal policy in the area of privacy.

In particular, the DoC's National Telecommunications and Information Administration (NTIA) on 25 September issued a request for comments on a proposed approach to consumer privacy. Comments were sought on elements such as transparency, security safeguards, risk management, accountability and ensuring that users are able to exercise control over their personal information and can reasonably access and correct their data. The Commision

services made a submission in response to this request for comments in November, which welcomes the NTIA's initiative and sets out the Commission's views on the elements of a modern data protection regime.[62]

In its submission, the Commission explained that the possible adoption of federal privacy legislation in the U.S. would strengthen the basis on which the Privacy Shield framework has been developed. In this regard, the Commission notably stressed the central importance of effective oversight and enforcement mechanisms. The Commission also underlined that the development of a federal regime on the basis of principles that are shared not only by the EU, but also by an increasing number of countries around the world, would strengthen the protections of our citizens when their data is transferred abroad. At the same time, it would help commercial operators navigate between different legal systems and offer new opportunities to facilitate trade.

In parallel to NTIA's request for public comments, the National Institute of Standards and Technology (NIST) is developing a Privacy Framework in collaboration with industry, civil society, academia, Federal agencies, etc. The Framework will be a voluntary tool for companies that could provide privacy outcomes and approaches to help companies with achieving privacy protection solutions.

Moreover, and as already explained above, the FTC has initiated a process of reflection on its current authority in the area of privacy which also looks into the efficacy of the FTC's use of its current remedial authority and the identification of any additional tools or authorities the FTC may need to adequately deter unfair and deceptive conduct related to privacy and data security.

Finally, the U.S. Senate held several hearings on consumer data privacy in the autumn of 2018: one hearing with major technology and communication companies took place on 26 September 2018[63] and a second hearing on a federal privacy law, in which Chair of the EDPB Andrea Jelinek participated, took place on 10 October 2018.[64]

As these developments are of 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.

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

[62] See https://ec.europa.eu/info/sites/info/files/european_commission_submission_on_a_proposed_approach_to_consumer_privacy.pdf

[63] See https://www.commerce.senate.gov/public/index.cfm/hearings?ID=2FF829A8-2172-44B8-BAF8-5E2062418F31

[64] See https://www.commerce.senate.gov/public/index.cfm/pressreleases?ID=2E7C60ED-9D88-418B-B5E0-EE2C41941E8C

Concerning the access and use of personal data transferred under the EU-U.S. Privacy Shield, the second annual review focused on relevant developments in the U.S. legal framework, including with respect to relevant agency policies and procedures, on recent trends as regards surveillance activities, and on developments in the setup and functioning of important oversight and redress bodies. Developments in U.S. case law concerning the availability of judicial redress in the area of government surveillance were equally assessed.

4.2.1. Access and use by U.S. public authorities for national security purposes

As set out in the adequacy decision[65] and confirmed by the first annual review[66], once personal data has been transferred to Privacy Shield-certified companies, U.S. intelligence authorities may only collect such data on the basis of the Foreign Intelligence Surveillance Act (FISA) or one of the statutes that authorise the use of so-called National Security Letters (NSLs). This was again confirmed by the ODNI and DoJ during the second annual review meeting.

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)[67], collection of personal data is always targeted.[68] Moreover, Presidential Policy Directive (PPD)-28 provides limitations and safeguards for the collection and use of signals intelligence that are specifically designed to protect non-Americans. At the first annual review meeting and again at the second annual review meeting, the U.S. authorities expressly confirmed that PPD-28 is fully effective and being implemented through policies and procedures of the individual intelligence agencies.[69]

It should also be noted that the U.S. Intelligence Community continues its efforts to provide transparency to the greatest extent possible. Additional documents have been declassified and published on the Internet, notably a summary of the FISA Amendments Reauthorization Act of 2017, recent opinions of the Foreign Intelligence Surveillance Court, a new Intelligence Community Directive on Civil Liberties, Privacy, and Transparency issued by the Director of National Intelligence, as well as recent Semiannual Assessments of Compliance with

[65] Recital 78 of the adequacy decision.
[66] See Section 4.2.1.2 of the Commission Staff Working Document.
[67] See recitals 71, 78-81 and sections 4.2.1.2 and 4.2.1.3 of the Commission Staff Working Document.
[68] 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. It should nevertheless be noted that in its recent judgment in Big Brother Watch and Others v. United Kingdom (application nos. 58170/13, 62322/14 and 24960/15, judgment of 13 September 2018) the European Court of Human Rights decided that bulk interception of communications is not *per se* a violation of the European Convention on Human Rights. Instead the Court recognised that bulk interception is a valuable means to achieve legitimate aims, particularly given the current threat level from both global terrorism and serious crime. It further determined that when assessing compliance with Article 8 of the Convention, the actual operation of the whole system of interception, including the checks and balances on the exercise of power, and the existence or absence of any evidence of actual abuse, would have to be taken into account. The case law of the Court thus confirms that the legality of bulk collection depends on the overall combination of the limitations and safeguards that are provided by the relevant legal system.
[69] See Section 4.2.1.1 of the Commission Staff Working Document.

Procedures and Guidelines Issued Pursuant to Section 702 of FISA jointly submitted by the Attorney General and the Director of National Intelligence. [70]

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

4.2.1.1.1. The re-authorisation of Section 702 FISA

Section 702 FISA is of particular relevance for the personal data of Europeans that have been transferred from the EU to Privacy Shield-certified companies in the U.S., as it authorises the acquisition of foreign intelligence information through the targeting of non-U.S. persons located outside the U.S. with the compelled assistance of U.S. electronic communication service providers. The FISA Amendments Act of 2008 which enacted Section 702 FISA was subject to a sunset clause and was therefore scheduled to expire at the end of 2017, unless re-authorised by Congress. After a first temporary re-authorisation without any changes, the FISA Amendments Reauthorization Act of 2017 was passed on 19 January 2018. The Act re-authorises Section 702 for six years, until 31 December 2023, but also introduces certain changes to Section 702 and other U.S. laws.

The Commission in its report on the first annual review of the Privacy Shield had expressed its hope that the U.S. Congress would consider favourably enshrining the protections offered by PPD-28 with respect to non-U.S. persons into FISA, with a view to ensuring the stability and continuity of these protections. While the protections of PPD-28 have not been included in Section 702 FISA, it is important to underline that there have been no amendments restricting the safeguards contained in FISA which were in place when the Privacy Shield decision was adopted. Moreover, the changes did not expand the powers of the U.S. Intelligence Community to acquire foreign intelligence information by targeting non-U.S. persons under Section 702. Instead, the FISA Amendments Reauthorization Act has expanded some privacy safeguards under FISA and other U.S. intelligence laws.

First, pursuant to the FISA Amendments Reauthorization Act, so-called "abouts" collection may no longer be carried out and may only be resumed under certain specific conditions. "Abouts" collection refers to the collection not only of communications *to* or *from* a Section 702 selector (such as an email address), but also of communications that contain a reference to such a selector (e.g. email communications which are not sent to or from the selected email address, but which include the selected email adress in the text or body of the email). [71] However, as also noted by several NGOs that the Commission consulted in preparation for the second annual review, the Act allows a possible future restarting of "abouts" collection, which is subject to strict conditions. According to this procedure, "abouts" collection can (again) be carried out if (i) it is authorized by the Foreign Intelligence Surveillance Court (FISC) and (ii) the intention to carry out "abouts" collection is notified to the relevant

[70] See http://icontherecord.tumblr.com/.

[71] "Abouts" collection had been carried out under the "upstream" collection program operated under Section 702 FISA, but the U.S. Intelligence Community had terminated this kind of collection in April 2017. This followed an order from the Foreign Intelligence Surveillance Court (FISC) which found that certain aspects of this type of collection were not in compliance with the minimization procedures approved by the FISC.

Committees in Congress and Congress does not act within 30 days of the notification. Congress would have to be provided with a written summary and explanation of the new program and would have to be convinced that the previous problems of compliance with minimization procedures have been solved. Congress may hold hearings and review the proposed collection. Prior to the FISA Court approving the government's request, the Act requests the FISA Court to consider appointing an *amicus curiae* to advocate for individual privacy and civil liberties interests during its review of the proposed collection.

While "about" collection was being carried out at the time when the Privacy Shield decision was adopted, its termination in April 2017 had lead to a reduction the intelligence collected.[72] It was confirmed at the second annual review that no steps are currently beeing taken within the Intelligence Community to restart "about" collection.

Second, while certain other important amendments concern U.S. persons only[73], a number of smaller changes bring improvements for all individuals.[74] In particular, the Director of National Intelligence (DNI) is now obliged to report each year the total number of Section 702 FISA targets and to make that number public as part of the DNI's annual Statistical Transparency Report. While the number of targets under Section 702 has been published since 2013 on a voluntary basis in the DNI's annual Statistical Transparency Report regarding the use of the national security authorities, this long-standing practice has now become a statutory requirement.

Third, the minimization procedures adopted for the handling of foreign intelligence information acquired under Section 702 have to be made publicly available to the greatest extent practicable. While mainly aimed at preventing the retention and dissemination of information concerning U.S persons, minimization procedures also provide protections for non-U.S. persons by restricting access to databases in which information is stored and by imposing limits on the use, retention and dissemination of such information. The NSA's minimization procedures had already been partially declassified and published on a voluntary basis in 2017. Under the FISA Amendments Reauthorization Act, this too has become mandatory.

Finally, two amendments to the enabling statute for the Privacy and Civil Liberties Oversight Board (PCLOB) allow the PCLOB to better exercise its advisory and oversight functions. First, the Act enables the serving members of the Board to exercise, by unanimous vote, the authority of the chairman to appoint staff if the position of chairman of the Board is vacant,

[72] See Section 4.2.1.3 of the Commission Staff Working Document.
[73] Queries of information collected under Section 702 that are designed to retrieve communications of or concerning U.S. persons have to be governed by querying procedures, which have to be reviewed and approved by the FISC. These procedures must include a record keeping of each U.S. person search term used. In addition, the use of U.S. persons' information obtained under Section 702 as evidence in a criminal procedure has been restricted. Moreover, the FBI must report the number of investigations opened by the FBI on U.S. persons based on information collected under Section 702.
[74] See also Summary of FISA Amendments Reauthorization Act of 2017, available at https://www.dni.gov/files/documents/icotr/Summary-FISA-Reauthorization-of-2017---10.15.18.pdf.

thereby ensuring that the PCLOB can continue to hire staff in order to fulfil its functions even in the absence of a chairman. Second, the Act enhances the PCLOB members' authority to meet and deliberate in private, helping them to assess government activity. Previously, the statute required the Board to comply with burdensome public meeting requirements designed for advisory boards not engaged in the review of sensitive government operations. While Board members could confer in closed session on certain matters (e.g. when classified information was involved), they were not otherwise permitted to confer with one another in private. At the same time , the PCLOB continues to be required to submit public reports and hold public hearings, also under the amended enabling statute.

It should also be noted that the NSA and the FBI have been added to the list of agencies that are required to appoint privacy and civil liberties officers. This is again a codification of a well-established practice, since these agencies have already been appointing privacy and civil liberties officers in the past without being legally obliged to do so.

4.2.1.1.2. PPD-28

As already noted, the U.S. authorities, represented by the ODNI, have confirmed at the second annual review meeting that PPD-28 remains in effect and is binding for the executive branch.[75]

Moreover, it should be noted that the PCLOB's Report to the President on "the Implementation of Presidential Policy Directive 28: Signals Intelligence Activities" has been publicly released on 16 October 2018.[76] Given the relevance of PPD-28 for the limitations and safeguards for non-U.S. persons applying to government access for signals intelligence, and thus for the Commission's periodic review of its adequacy assessment, the Commission in its report on the first annual review had called on the U.S. administration to make this report available to the public.

The PCLOB report is based on classified briefings and discussions with elements of the Intelligence Community. The PCLOB also examined the policies that implement PPD-28 within and across the different elements of the Intelligence Community and took into account public comments, primarily from NGOs. The report confirms that PPD-28 is fully applied across the Intelligence Community. Further to the issuance of PPD-28, the relevant elements of the Intelligence Community have adopted detailed rules on the implementation of PPD-28 and have significantly changed their practices in order to bring them in line with the requirements of PPD-28 regarding the collection, use, retention and dissemination of signals intelligence information.

[75] The ODNI further explained that the Trump Administration conducted a review of PPD-28 (which had been issued in 2014 by President Obama) in 2017, and determined that it should remain in place.
[76] Under Section 5(b) of PPD-28, the PLCOB is encouraged to provide the President with a report that assesses the implementation of the Directive. The PCOB's report pursuant to Section 5(b) of PPD-28 was adopted unanimously on 14 December 2016. It is available at https://www.pclob.gov/reports/report-PPD28/.

At the same time, it results from the report that at least for a certain period of time (it should be kept in mind that the report was adopted in December 2016), the interpretation of PPD-28 varied between the different elements of the Intelligence Community, due to some uncertainty as to the question regarding which surveillance activities qualify as signals intelligence and are therefore subject to the protections of PPD-28.[77] Yet the report also clearly confirms that despite this uncertainty, the NSA, CIA and FBI did apply PPD-28 to communications collected under Section 702 FISA. In other words, it appears that the questions around the exact delineation of the notion of signals intelligence did not have an impact in practice on the safeguards that apply to non-U.S. persons. In addition, in its response to the PCLOB's report of October 2018, the ODNI explicitly confirmed that "*it is the current official position of the United States Government (including the IC) that PPD-28 applies to collection under Section 702 of FISA*".[78] At the second annual review, the ODNI also explained that since the PCLOB's report was adopted already in 2016 but subject to presidential privilege and released only recently, some of the initial uncertainties regarding the application of PPD-28 had in the meantime been addressed, in particular as the ODNI had worked with the different agencies in order to ensure a consistent application. At the second annual review meeting, the ODNI also confirmed its readiness to work with the newly appointed PCLOB to follow-up on the report.

The confirmation by an independent oversight body such as the PCLOB that the relevant intelligence agencies do effectively apply PPD-28 to the collection of intelligence information under Section 702 and implement its provisions both through the adoption of detailed agency rules and in practice is an important piece of information for the assessment of the functioning of the Privacy Shield framework, as PPD-28 extends certain protections under FISA, amongst others, to foreigners, which would otherwise be limited to U.S. persons only.[79]

4.2.1.1.3. The CLOUD Act

The United States CLOUD Act adopted by the United States Congress on 23 March 2018[80], amends the Stored Communications Act of 1986 in that U.S. service providers are obliged to comply with United States orders to disclose content and other data, regardless of where such data is stored. It also establishes a framework for the conclusion, under certain conditions, of executive agreements with foreign governments, on the basis of which United States service providers would be allowed to disclose content data directly to law enforcement authorities of these third countries in investigation of serious crime, subject to civil liberties and privacy limitations and safeguards to be part of executive agreements.

[77] PPD-28 sets out principles and limitations that govern the use and collection of "signals intelligence activities". However, PPD-28 does not define "signals intelligence activities".
[78] Status of Implementation of PPD-28: Response to the PCLOB's Report –October 2018, p.5, available at http://icontherecord.tumblr.com/post/179122454368/status-of-implementation-of-ppd-28-response-to.
[79] PPD-28 extends to non-U.S. persons the protections provided for U.S. persons with respect to the retention and dissemination of data.
[80] Clarifying Lawful Overseas Use of Data Act, H.R. 4943.

The adoption of the CLOUD Act has raised some concerns, notably among the NGOs that the Commission consulted in preparation of the second annual review. In particular, some NGOs are of the view that the protections required for executive agreements under the CLOUD Act granting foreign access to data stored in the U.S. are not sufficient.

The CLOUD Act addresses the question that was the subject of the *Microsoft* case[81], i.e. whether on the basis of a warrant issued by a U.S. court, a U.S. provideris required to disclose data that is stored outside of the U.S. The CLOUD Act thus clarifies that U.S. law enforcement can request data stored outside of the U.S., whereas the Privacy Shield concerns only personal data that is processed within the U.S. after it has been transferred from the EU. However, the CLOUD Act could in the future become relevant for the Privacy Shield, as far as it also allows the conclusion of executive agreements with international partners that give foreign governments access to data stored in the U.S., potentially by Privacy Shield-certified companies. Yet the CLOUD Act subjects the conclusion of such executive agreements to a number of safeguards and requirements: the foreign domestic law and its implementation must provide sufficient substantive and procedural protections for privacy and civil liberties (in particular the law needs to provide clear legal mandates and procedures for requesting data under the executive agreement, including for the collection, retention, use, and sharing of data), and effective oversight of these activities; orders must be limited to address serious crimes, comply with the foreign domestic law, be specifically targeted and be subject to independent review or oversight. Moreover, Congress has the possibility to object to the executive agreement. These limitations should help to ensure that any future agreement would be in line with the requirements of the Privacy Shield. In addition, there will only be a concrete impact on the protections offered by the Privacy Shield once the first executive agreements have been concluded. The Commission will therefore closely monitor whether any executive agreements under the CLOUD Act are being concluded and, should that be the case, carefully assess their concrete impact on the Privacy Shield.

4.2.1.2. Surveillance activities in practice: figures and trends

The ODNI's Statistical Transparency Report Regarding Use of National Security Authorities for calendar year 2017 shows that the number of targets under Section 702 FISA increased from 106,469 in CY2016 to 129,080 in CY2017. In addition, the number of NSLs issued increased slightly from 12,150 in CY2016 to 12,762 in CY2017.

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.

[81] United States v. Microsoft Corp., No. 17-2, 584 U.S. (2018).
[82] USA FREEDOM Act of 2015, Pub. L. No 114-23, Section 602(a), 603(a).

When compared with last year's figures[83], the numbers published by companies mirror the moderate increase in requests under FISA that is identified in the ODNI's Statistical Transparency Report. For example, during the reporting period July 2017 to December 2017, Google received between 500 and 999 requests for access to content under FISA, affecting between 48 500 and 48 999 users, and between 4 and 499 NSL requests, affecting between 1500 and 1999 users.[84] Facebook received between 0 and 499 requests for access to content under FISA, affecting between 20 000 and 20 199 accounts, during the reporting period June to December 2017.[85] From July to December 2017, Facebook received between 0 and 499 NSL requests, affecting between 1 and 499 accounts.[86].

At the second annual review meeting, the U.S. authorities explained that from the point of view of the bodies responsible for the oversight of the intelligence community, the increase in the number of Section 702 targets and NSLs issued, as reported by ODNI in its Statistical Transparency Report, was not considered to be particularly significant. According to the explanations provided during the second annual review meeting, there are several factors that could explain this increase, including certain events that occurred in the course of the last year, e.g. actions by certain nation state actors or certain cyberattacks. The U.S. authorities also highlighted that there are around 2.3 billion Internet users outside of the US., which means that only 0.005% of them are targeted by U.S. electronic surveillance.

4.2.1.3. Independent oversight

4.2.1.3.1. Inspectors General

At this year's annual review meeting, the Inspector General for the Intelligence Community was present in person. He gave an overview of an Inspector General (IG)'s tasks and powers, which confirmed the findings of the first annual review,[87] and explained in more detail his own role and mission.

He notably confirmed that IGs are independent by design and by law, and their removal would be most unusual.[88] As regards the IG's access to documents, he explained that access can be both indirect (i.e. through the relevant government authority) or direct (e.g. because of the way the electronic systems are arranged or in cases where indirect access is considered inadequate). To the Inspector General's knowledge, the IG for the Intelligence Community had never been denied access to records and if access were to be denied, Congress would have to be informed.

The Office of the IG for the Intelligence Community employs 73 staff members, while other IG offices, for example the one of the Department of Defense, are significantly larger. The IG

[83] See Section 4.2.3.1 of the Commission Staff Working Document.
[84] https://transparencyreport.google.com/user-data/us-national-security?hl=en
[85] https://transparency.facebook.com/government-data-requests/country/US/-jul dec-2017
[86] https://transparency.facebook.com/government-data-requests/country/US/-jul dec-2017
[87] See Commission Staff Working Document, section 4.2.2, p. 29-30.
[88] Only the President can remove an IG, and "for cause" only. If an IG is removed from office, Congress has to be informed.

of the Intelligence Community relies mostly on reports of wrongdoing in order to identify areas that require an investigation, but he can also use his discretion to identify issues for review. Importantly, the Inspector General confirmed that any referral from the Privacy Shield Ombudsperson would receive his "*serious, timely and effective attention*".

The Inspector General also explained the IG's activities with respect to the protection of whistleblowers. The IG of the Intelligence Community offers a dedicated telephone hotline and email address (in both cases with separate channels for submitting classified information) through which wrongdoing can be reported. In the framework of a whistleblower reporting group within the Intelligence Community, best practices in case of allegations of reprisals against whistleblowers are being discussed with a view to assisting the persons concerned.

4.2.1.3.2. The Privacy and Civil Liberties Oversight Board

At the time of the first annual review, four of the PCLOB's five seats were vacant, with only one Board member remaining. In its report on the first annual review, the Commission recommended the swift appointment of the missing members of the PCLOB to ensure that the Board would be able to fulfil all aspects of its function. On 13 March 2018, the White House announced the nomination of Edward Felten and Jane Nitze to serve as members of the PCLOB. Furthermore, on 7 August 2018, President Trump announced his intent to nominate Aditya Bamzai and Travis LeBlanc to be members of the PCLOB.

On 11 October 2018, the Senate confirmed the nominations of Adam Klein (who was nominated Chairman of the PCLOB on 5 September 2017), Edward Felten and Jane Nitze. The Commission services welcome that, with these confirmations, the Board has regained its quorum and can fully exercise all of its functions.

Newly appointed Chairman Adam Klein and member Edward Felten participated in person in the second annual review meeting. They presented the history, role and tasks of the PCLOB, which confirmed the Commission's findings in the adequacy decision and the report on the first annual review.[89]

With respect to ongoing oversight projects, it was clarified that the PCLOB in the context of its examination of E.O. 12333 is carrying out in-depth examinations of three counter terrorism programs, one at the NSA and two at the CIA. The examination of one of the CIA's activities had been finalised in 2016, but the report is classified. The new Board will review the report and, if deemed appropriate, work with the Intelligence Community on a declassified version. Moreover, the Board is currently looking into data aggregation and open source data and will continue its work in these areas.

As regards a potential update of the PCLOB's report on Section 702 that was adopted in 2014, Chairman Klein clarified that the PCLOB in 2016 issued an assessment report to analyse the implementation of its recommendations concerning FISA, including Section

[89] See recital 98 of the adequacy decision and Commission Staff Working Document, section 4.2.3.2, p. 30-31.

702.[90] While Chairman Klein was in favour of updating this assessment, he explained that such decision would need to be taken by the Board as a whole. The Commission strongly encourages the issuance of such a report as it is a very valuable source of information, and will closely monitor any developments in this regard.

4.2.1.4. Individual redress

4.2.1.4.1. The Privacy Shield Ombudsperson mechanism

After the first annual review, the Commission had come to the conclusion that the Ombudsperson mechanism was in place and ready to function as intended in the adequacy decision. At the same time, given the importance of the Ombudsperson mechanism for the Privacy Shield framework, it had recommended the swift appointment of a permanent Privacy Shield Ombudsperson.

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. On 28 September 2018, Manisha Singh, a senior official in the State Department, had been designated by President Trump as Acting Under Secretary of State that includes the role of acting Privacy Shield Ombudsperson,[91] but it was not yet clear when the post would be permanently filled. While the acting Ombudsperson continues to carry all functions under the Ombudsperson mechanism, the absence of a permanent appointee is highly unsatisfactory and should be remedied as soon as possible. In that regard, the Commission took note of the fact that at the second annual review, the U.S. government recognised the need for prompt progress on nominating a permanent Under Secretary and confirmed that this process is well underway.

In her presentation at the second annual review meeting, Ms. Singh emphasised that her appointment reflects the full commitment of President Trump and Secretary of State Pompeo to the Ombudsperson mechanism. She explained that in her role of acting Ombudsperson, she is fully empowered to carry out all relevant functions. Ms. Singh also confirmed that the mechanism is fully prepared to handle any complaints. Given that no complaint had been lodged by the time of the second annual review, it was explained in detail how a hypothetical case would be handled by the Ombudsperson, which corresponded with the findings of the first annual review regarding the Ombudsperson's procedure for handling complaints.[92]

In particular, when asked about her powers to access information and to remedy potential violations, Ms. Singh confirmed that she has the possibility to obtain all the information she needs and that she has the necessary tools at her disposal to ensure that any incident is properly remedied. If she was not satisfied with the cooperation and/or remedy provided, she

[90] Privacy and Civil Liberties Oversight Board, Recommendations Assessment Report, 5 February 2016, available at https://www.pclob.gov/library/Recommendations_Assessment_Report_20160205.pdf .
[91] Her predecessor in the function of Ombudsperon, Ambassador J. Garber, had been acting Assistant Secretary (see Commission Staff Working Document, section 4.2.4.2, p. 34). Ms. Singh has been designated acting Under Secretary and therefore holds a higher position in the Department of State.
[92] See Commission Staff Working Document, section 4.2.4.2, p. 34-36.

would also have the possibility to elevate the matter to the Secretary of State, to whom she reports directly. Importantly, the General Counsel of the ODNI confirmed that as a matter of good governance, the Intelligence Community was fully committed to cooperating with the Ombudsperson. It was also confirmed that the relevant Privacy and Civil Liberties Officer and the independent Inspector General of the Intelligence Community would always be closely involved, including by receiving a copy of the complaint.

The representatives of the EDPB participating in the second annual review explained how a complaint to the Ombudsperson is handled on the EU side. In fact there is a two-step approach: a request has to be directed first to a national DPA, i.e. the DPA of the citizen's country of residence, and the DPA checks the completeness of the requests and asks for additional information, if necessary (e.g. copy of ID document to prove the identity of the complainant, etc.). Once the DPA deems the request complete, it refers it to the EU Individual Complaint Handling Body, also being referred to as EU Centralised Body, which was first the Article 29 Working Party and is now the EDPB, where five DPAs (France, Austria, Germany, Bulgaria and UK) conduct an additional review on behalf of the EDPB. After this further check, the complaint is transmitted to the Ombudsperson mechanism via the online platform that has been created for this purpose. The EU Centralised Body has created a single email address which serves as a central contact point both for referrals of requests from national DPAs and for correspondence with the team of the Ombudsperson mechanism within the Department of State.

At the time of the second annual review, the Ombudsperson mechanism had not yet received any requests. However, a request to the Ombudsperson had been submitted to the Croatian DPA and the relevant checks were ongoing. If found complete and submitted to the Ombudsperson for investigation and follow-up, this would allow the Commission services to better assess the functioning of the Ombudsperson mechanism in practice, most probably at the next annual review. The Commission will therefore closely monitor the developments in this respect, including the timeframe in which this complaint is being handled.[93]

4.2.1.4.2. Judicial remedies available to EU individuals

As regards the redress possibilities identified in the adequacy decision[94] and further discussed during the first annual review,[95] there have been no significant developments in the U.S. case law. Several cases concerning surveillance under Section 702 FISA brought under the Administrative Procedure Act[96] are still pending before the U.S. courts. The Commission services will continue to closely monitor any developments in this respect.

In the adequacy decision and during the first annual review, it was confirmed that the Freedom of Information Act ("FOIA")[97] is an important instrument that is increasingly used

[93] The Ombudsperson is required to provide an appropriate response *"in a timely manner"*. See Section 4e, Annex A to Annex III of the adequacy decision.
[94] Recitals 111-124 of the adequacy decision.
[95] See Commission Staff Working Document, section 4.2.4.1., p. 32-33.
[96] Recitals 113, 131 of the adequacy decision and Commission Staff Working Document, section 4.2.4.1, p. 32.
[97] Recitals 114, 133 of the adequacy decision and Commission Staff Working Document, section 4.2.4.1, p. 32.

by individuals to seek access to records held by federal agencies. Since the first annual review, a significant number of additional documents related to orders and opinions by the FISC has been made publicly available on the basis of requests pursuant to FOIA.[98] The publication of these documents which provide information on how the FISC oversees certifications (including by publishing copies of certifications, written questions on Section 702 FISA, responses from government agencies on how they use procedures under FISA, etc.) is an important contribution to transparency in the area of national security.[99]

In one case before the FISC that concerned the question of standing, three public interest groups requested access to classified parts of FISC opinions on the basis of the First Amendment right of access. Their motion was initially denied on the ground that, since the interest groups failed to claim an injury or legally protected interest, they lacked standing. This decision was overruled by a decision of 16 March 2018, in which the Foreign Intelligence Surveillance Court of Review found that the interest groups in this case met the standing threshold, since the injury in this case was the denial of access to FISC opinions and the applicants demonstrated that their claimed right of access was judicially cognizable.[100] While this decision does not concern the standing requirement in the context of a specific surveillance program and does not deal with the merits of the request, it indicates that under FOIA there is no requirement to demonstrate standing other than showing that access to government documents was denied.

4.2.2. Access and use by U.S. public authorities for law enforcement purposes

Since the first annual review, there have been two relevant developments in the area of access to personal data for law enforcement purposes. In particular, the protections of individuals have been strengthened through an important Supreme Court ruling and by an initiative of the executive branch.

In the case of *Carpenter v. United States*[101], the U.S. Supreme Court held that a search warrant is in principle required for law enforcement authorities to access cell site location records. In *Carpenter*, U.S. law enforcement had obtained cell site location data on the basis of a court order for disclosure, which requires reasonable grounds to believe that the information is relevant and material to an ongoing criminal investigation. The Supreme Court held that the U.S. authorities conducted a search under the Fourth Amendment of the U.S. Constitutions when accessing cell site location records. According to the *Carpenter* judgment, historical cell site location records can provide a comprehensive overview of a user's movements and the user has the reasonable expectation of privacy with respect to this information. As a consequence, a search warrant under the Fourth Amendment to the U.S.

[98] See releases of 25 September 2017, 31 January 2018 and 22 August 2018 based on EFF FOIA litigation, http://icontherecord.tumblr.com/post/165800143933/release-of-fisa-title-iv-and-v-documents and release of 11 October 2017 based on NYT FOIA litigation, http://icontherecord.tumblr.com/post/58944252298/dni-declassifies-intelligence-community-documents.
[99] See also above, Section 4.2.1.
[100] FISCR 18-01 Opinion, 16 March 2018.
[101] Timothy Ivory Carpenter v. United States of America, No. 16-402, 585 U.S. (2018).

Constitution, which requires showing the existence of probable cause (and is therefore more difficult to obtain), is required to obtain cell site location records.

Fourth Amendment rights generally only apply to individuals with a substantial connection to the U.S.,[102] but as also pointed out by the NGOs that replied to the Commission's questionnaire, the *Carpenter* judgment shows the evolving jurisprudence of the U.S. courts in the area of privacy in light of technological developments.[103] This seems to demonstrate how the Supreme Court adapts traditional privacy protections to the challenges of the digital era.

Another key development concerns a memorandum issued by Deputy Attorney General Rod Rosenstein on 19 October 2017 to U.S. attorneys and agents on a more restrictive policy on applications for protective (or non-disclosure) orders pursuant to 18 U.S.C. § 2705(b) of the Stored Communications Act ("SCA"). This guidance document applies to all applications seeking protective orders filed on or after 30 days of the issuance of the memorandum. According to the SCA, the U.S. authorities, on the basis of a warrant, subpoena or court order, can obtain records and information relating to customers or subscribers from providers of electronic communications services or remote computing services (both content and non-content data).

Providers are able to voluntarily notify a customer or subsriber whose information is sought by law enforcement authorities except when such authorities obtain a protective order prohibiting voluntary notification. Such a protective order is a court order commanding a provider of electronic communications services or remote computing services to whom a warrant, subpoena or court order is directed, not to notify any other person of the existence of the warrant, subpoena or court order, for as long as the court deems appropriate. Protective orders are granted if a court finds that there is reason to believe that notification would seriously jeopardise an investigation or unduly delay a trial, e.g. because it would result in endangering the life or physical safety of an individual, flight from prosecution, intimidation of potential witnesses, etc.

The purpose of the memorandum is to harmonise the current practice of applications for protective orders and set a general ceiling on how long a notification can be withheld. To this end, the memorandum requires prosecutors to make a detailed determination regarding the need for a protective order and provide a justification to the court on how the statutory criteria for obtaining a protective order are met in the specific case. The memorandum also requires that applications for protective orders must generally not seek to delay notification for more than one year. It is further specified that, where, in exceptional circumstances, orders of longer duration might be necessary, such orders may only be sought with the written agreement of a supervisor designated by the U.S. Attorney or the appropriate

[102] Non U.S. persons that are not resident in the U.S. benefit indirectly from the Fourth Amendment protections, given that personal data is being held by U.S. companies with the effect that law enforcement authorities in any event have to seek judicial authorisation to access this data. See recital 127 of the adequacy decision.

[103] This is also seen in other case law, for example in a case of 2014, where the Supreme Court ruled (Riley v. California, 573 U.S. (2014)) that a search warrant under the Fourth Amendment is required for law enforcement authorities to seize and search a cell phone, given the *"immense storage capacity of modern cell phones*".

Assistant Attorney General. The memorandum is binding for all DoJ attorneys and agents (which include federal prosecutors).

During the second annual review meeting, the DoJ confirmed that this memorandum contributes to increased transparency and prevention of overuse of protective orders: the requirement to justify the reason for seeking a protective order will act as an additional filter, while the one-year limitation harmonises the current practice and sets a clear boundary for applications for protective orders. Since the memorandum provides guidance only on the application for protective orders and not for the final court assessment, the U.S. courts could in principle grant protective orders for longer than one year. The DoJ confirmed that this discretion remains with the courts, but that, in practice, a court would normally not go beyond the prosecutor's request. By providing additional conditions and a clear time limit for applications that seek to delay the notification of individuals, the DoJ's new policy contributes to stronger protections where law enforcement authorities seek to obtain access to personal data transferred under the Privacy Shield. In particular, the notification of individuals when law enforcement authorities request access to their personal data is an important element to help individuals to obtain judicial redress by showing individual concern and thus demonstrate "standing".