

**From:** [REDACTED] (JUST)  
**Sent:** 22 July 2016 05:56  
**To:** [REDACTED] (JUST); [REDACTED] (JUST)  
**Subject:** Fwd: Pricing structure

**Follow Up Flag:** Follow up  
**Flag Status:** Flagged

Inviato da iPhone

(Inizio messaggio inoltrato)

**Da:** [REDACTED]@trade.gov>  
**Data:** 22 luglio 2016 10:15:48 GMT+8  
**A:** "[REDACTED] (EC)" [REDACTED]@ec.europa.eu>  
**Oggetto:** Pricing structure

This is not yet public, but will be released tomorrow or Monday.

Organization's Annual Revenue	Annual Fee:
\$0 to \$5 million	\$250
Over \$5 million to \$25 million	\$650
Over \$25 million to \$500 million	\$1,000
Over \$500 million to \$5 billion	\$2,500
Over \$5 billion	\$3250

Sent from my BlackBerry 10 smartphone on the Verizon Wireless 4G LTE network.



**UNITED STATES DEPARTMENT OF COMMERCE**  
**The Secretary of Commerce**  
Washington, D.C. 20230

August 8, 2016

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

Dear Commissioner Jourová:

Congratulations on the successful approval of the EU-U.S. Privacy Shield Framework. I would like to thank you again for your tireless commitment and dedication to working with me throughout the past two years. This Framework is a testament to the enduring strength of our transatlantic partnership.

It was a pleasure to meet with you in Brussels before the Privacy Shield press conference to celebrate this momentous occasion. I appreciated our discussion of the next phase of this process as we shift our focus to implementation. The Department of Commerce's newly launched web site (which you can visit at <https://www.privacyshield.gov>) is the most visible example of our implementation work. I am pleased to report that we have also expanded the Privacy Shield team and are already hard at work on the Framework's implementation.

My staff and I look forward to continuing this work together to ensure that the Privacy Shield is a success and that it protects privacy as intended.

The Department of Commerce also takes our commitment to increased outreach very seriously. As we discussed in Brussels, we would like to conduct this outreach alongside the European Commission where possible. I am glad that our teams are already exploring opportunities to make this happen. I look forward to our ongoing engagement on this and other issues.

Again, please accept both my congratulations and my gratitude on this momentous occasion.

Sincerely,

A handwritten signature in dark ink, reading "Penny Pritzker".  
Penny Pritzker

From: [REDACTED] (JUST)  
Sent: 12 September 2016 17:54  
To: [REDACTED] (USEU)  
Cc: [REDACTED] (JUST)  
Subject: RE: Question

Follow Up Flag: Follow up  
Flag Status: Flagged

[REDACTED]

Where, on the basis of the checks or of any other information available, the Commission concludes that the level of protection offered by the Privacy Shield can no longer be regarded as essentially equivalent to the one in the Union, or where there are clear indications that effective compliance with the Principles in the United States might no longer be ensured, or that the actions of U.S. public authorities responsible for national security or the prevention, investigation, detection or prosecution of criminal offenses do not ensure the required level of protection, it will inform the Department of Commerce thereof and request that appropriate measures are taken to swiftly address any potential non-compliance with the Principles within a specified, reasonable timeframe. If, after the expiration of the specified timeframe, the U.S. authorities fail to demonstrate satisfactorily that the EU-U.S. Privacy Shield continues to guarantee effective compliance and an adequate level of protection, the Commission will initiate the procedure leading to the partial or complete suspension or repeal of this decision.<sup>208</sup>

-----Original Message-----

From: [REDACTED] (USEU) [REDACTED]@state.gov  
Sent: Monday, September 12, 2016 1:25 PM  
To: [REDACTED] (JUST)  
Cc: [REDACTED] (JUST)  
Subject: RE: Question

Thanks. That is what i thought -- it is just that in English the "will" vs. "may" led me to double check. Notwithstanding the opinions of other institutions, my understanding is correct that given that we knew the gdpr's provisions at at time of finalisation of PS that the Commission does not expect to use such powers absent significant intervening circumstances, yes?

---

From: [REDACTED]@ec.europa.eu [REDACTED]@ec.europa.eu>  
Date: 12 September 2016 at 13:01:26 GMT+2  
To: [REDACTED] (USEU) [REDACTED]@state.gov>

Cc: [REDACTED]@ec.europa.eu [REDACTED]@ec.europa.eu>  
Subject: RE: Question

Hi [REDACTED]

No, that is not the intention. The "will make use of its powers" is perhaps not a perfect formulation, but it just means that the COM could - if there was a need and the conditions are fulfilled - make use of the urgency procedure under the GDPR for suspending the PS decision.

So if there was a need for such a suspension - which obviously is not a step that would be taken lightly - the Commission would not necessarily have to wait for prior "authorisation" by the Article 31 (comitology) Committee but could take an "interim" decision (if the conditions under the GDPR are fulfilled), followed by a consultation of that committee.

Hope that clarifies.

Best,  
[REDACTED]

Fn. 208:

As of the date of application of the General Data Protection Regulation, the Commission will make use of its powers to adopt, on duly justified imperative grounds of urgency, an implementing act suspending the present decision which shall apply immediately without its prior submission to the relevant comitology committee and shall remain in force for a period not exceeding six months.

-----Original Message-----

From: [REDACTED] (USEU) [REDACTED]@state.gov]  
Sent: Monday, September 12, 2016 12:39 PM  
To: [REDACTED] (JUST)  
Subject: RE: Question

PS - if this was discussed during the negotiations my apologies: i either do not recall or was not involved.

---

From: [REDACTED] (USEU) [REDACTED]@state.gov<mailto:[REDACTED]@state.gov>>  
Date: 12 September 2016 at 12:37:54 GMT+2  
To: [REDACTED]@ec.europa.eu<[REDACTED]@ec.europa.eu>  
[REDACTED]@ec.europa.eu<[REDACTED]@ec.europa.eu>>  
Subject: RE: Question

Hello. No worries. I was looking at the PS adequacy decision and realized i was not quite sure what to make of footnote 208.

Can you explain its meaning? On its face it appears to limit PS to between now and GDPR effective/implementation date.

Thanks  
[REDACTED]

---

From: [REDACTED]@ec.europa.eu<[REDACTED]@ec.europa.eu>  
[REDACTED]@ec.europa.eu<[REDACTED]@ec.europa.eu>>  
Date: 12 September 2016 at 08:41:27 GMT+2  
To: [REDACTED] (USEU) [REDACTED]@state.gov [REDACTED]@state.gov>>  
Subject: RE: Question

Hi [REDACTED]

Sorry, was away and busy with the duties of a best man... so I saw your email too late.

Still worth talking about?

Best,  
[REDACTED]

From: [REDACTED] (USEU) [REDACTED]@state.gov]  
Sent: Friday, September 09, 2016 2:28 PM  
To: [REDACTED] (JUST)  
Subject: Question

[REDACTED]  
Are you around for a quick chat? I had a clarifying question on one aspect of the PS adequacy decision.

Thanks  
[REDACTED]

[REDACTED]  
U.S. Mission to the European Union  
Brussels  
[REDACTED]

This email is UNCLASSIFIED.

**VĚRA JOUROVÁ**  
*Member of the European Commission*

Ref. Ares(2016)5498641 - 22/09/2016

Brussels,  
Ares(2016)

Dear Secretary Pritzker,

Thank you very much for your letter of 8 August 2016.

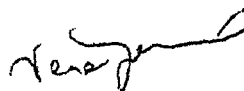
The Privacy Shield, running now in the second month, is our common achievement and as you noted in your letter, our focus should now be on its full implementation. The long-lasting success of this framework will of course depend to a large extent on compliance by companies with their commitments. This begins with the ongoing certification process which requires an in-depth assessment of companies' privacy policies. Subsequently, as agreed, a close eye should be kept on companies' compliance with the Privacy Principles, including pro-active monitoring.

As we briefly discussed in July in Brussels, a number of open issues need to be addressed to ensure full implementation of the framework. This concerns in particular:

- The Privacy Shield arbitration panel: we need to set out appropriate procedural rules, decide on funding and appoint the arbitrators.
- The Ombudsperson mechanism: I understand that the mechanism is being made operational by putting in place procedures and dedicating resources for the handling and resolution of individual complaints (on our side, we are in the process of designating an "EU centralised body" which will channel complaints to the Ombudsperson). In this regard, I would very much welcome some more information on the establishment and functioning of the Ombudsperson office, including on its cooperation with independent oversight bodies.
- Referral procedures (DPAs/DoC; DoC/FTC): I believe that putting in place standardised referral procedures could help to ensure the efficient handling and cross-referral of complaints within the agreed time limits.
- Annual reviews: I believe that we should soon start preparing for the first joint review, including agreeing on how these reviews will be carried out.

Bearing these points in mind, I look forward to continuing working together with you to ensure that the Privacy Shield serves our citizens and businesses to the fullest.

Yours sincerely,



Věra Jourová

Mrs Penny Pritzker  
Secretary of Commerce  
United States Department of Commerce  
Washington, D.C. 20230

Electronically signed on 22/09/2016 at 10:30 (C+02) in accordance with article 4.2 (Validity of electronic documents) of Commission Decision 2004/563



EUROPEAN COMMISSION  
DIRECTORATE-GENERAL JUSTICE and CONSUMERS

Director-General

Brussels,  
DG JUST/C4/RS/im Ares(2016)

Mr Kenneth E. Hyatt  
Acting Under Secretary for  
International Trade, United States  
Department of Commerce,  
International Trade Administration,  
Washington D.C. 20230, USA

Dear Mr Hyatt,

Under the European Commission's decision on the EU-U.S. Privacy Shield, adopted on 12 July 2016 and published in the EU Official Journal on 1 August 2016, the Commission has committed to continuously monitor the functioning of the framework with a view to assessing whether the United States continues to ensure an adequate level of protection of personal data transferred from the European Union to Privacy Shield-certified U.S. organisations. This monitoring includes any indications that interferences by U.S. public authorities responsible for national security and/or law enforcement with the right of Europeans to the protection of their personal data go beyond what is strictly necessary and/or that there is no effective legal protection against such interferences.

In recent days, the Commission has become aware of media reports on possible monitoring activities carried out by Yahoo with respect to email traffic on its network and in response to a request issued by an unnamed U.S. intelligence agency (or agencies). These activities were first reported by Reuters on 4 October 2016<sup>1</sup> and have since been picked up – with different accounts as to the specific facts – by other media outlets, including in an article by The New York Times of 5 October that was apparently based on information from U.S. government sources.<sup>2</sup>

---

<sup>1</sup> Reuters, 'Yahoo secretly scanned customer emails for U.S. intelligence-sources', 4 October 2016, available at: <http://www.reuters.com/article/us-yahoo-nsa-exclusive-idUSKCN1241YT>. Subsequently, Reuters adapted its initial report.

<sup>2</sup> The New York Times, 'Yahoo Said to Have Aided U.S. Email Surveillance by Adapting Spam Filter', 5 October 2016, available at: [http://www.nytimes.com/2016/10/06/technology/yahoo-email-tech-companies-government-investigations.html?\\_r=0](http://www.nytimes.com/2016/10/06/technology/yahoo-email-tech-companies-government-investigations.html?_r=0).

While not confirming the veracity of these reports, in response to questions both the White House Press Secretary and the Office of the Director of National Intelligence's Public Affairs Deputy Director have stressed that "*Under FISA, activity is narrowly focused on specific foreign intelligence targets and does not involve bulk collection or the use of generic key words or phrases.*" Admiral Rogers, the Director of the NSA, is reported as having stated that "*[w]e have to make a specific case. What the [FISA] court grants is specific authority for a specific period of time for a specified purpose.*"

Given that these reports suggest interference by U.S. public authorities with the right of Europeans to the protection of their personal data when these are transferred to the United States, the Commission needs to better understand how the reported activities would fit with the assurance provided by the U.S. government in the context of the Privacy Shield. This concerns in particular the specific representations contained in the two letters by the General Counsel of the Office of the Director of National Intelligence<sup>3</sup> which cover all U.S. signals intelligence activities.

The Commission would be particularly interested in obtaining clarifications on the following aspects:

- Do the reported activities (also) concern personal data transferred from the EU to the United States?
- Are the reported activities on-going or, if not, during which period have they been carried out? Have other U.S. companies that process the personal data of Europeans been subjected to similar requests by U.S. public authorities?
- How would the U.S. government qualify the reported activities (what is the magnitude of the monitoring activities by Yahoo? in the view of the U.S. government, does this constitute targeted or bulk collection?)
- How do the reported activities fit with the assurance received from the U.S. government, in particular, that: (i) the United States does not engage in "mass" or "indiscriminate" collection of data; (ii) "whenever practicable, signals intelligence collection activities are conducted in a targeted manner rather than in bulk" and bulk collection will only be carried out when targeted collection is not possible "due to technical or operational considerations"; (iii) the U.S.A. Freedom Act prohibits bulk collection pursuant to various provisions of FISA; (iv) even when targeted collection is not possible, the U.S. "applies filters and other technical tools to focus its collection on those facilities that are likely to contain communications of foreign intelligence value", "while minimizing the collection of non-pertinent information".

In addition, the Commission would be interested to receive information on what legal basis the reported activities have been (or are) carried out, whether they have been

---

<sup>3</sup> These letters form part of the Privacy Shield Package transmitted to the Commission by U.S. Secretary of Commerce Penny Pritzker and have been attached to the Commission's Privacy Shield adequacy decision as Annex VI.



authorised by way of a court decision and, if so, whether that decision involves a novel interpretation of U.S. intelligence laws or the U.S. Constitution and will therefore be declassified (so that it could be made available to the Commission). This would also be in line with the DOC's commitment to make reasonable efforts to inform the Commission of material developments in the law in the United States so far as these are relevant to the limitations and safeguards applicable to access to personal data by U.S. authorities and its subsequent use.

Thank you in advance for your support in this matter, clarification of which is of great importance for the administration of the Privacy Shield.

Yours sincerely,



Tiina ASTOLA

Cc: Catherine A. Novelli, Under Secretary of State for Economic Growth, Energy, and the Environment, U.S. Department of State

Robert S. Litt, General Counsel, Office of the Director of National Intelligence

Kevin O'Connell, Paul Nemitz, [REDACTED]



**UNITED STATES DEPARTMENT OF COMMERCE**  
**The Secretary of Commerce**  
Washington, D.C. 20230

October 27, 2016

Ms. Věra Jourová  
Commissioner for Justice, Consumers  
and Gender Equality  
European Commission  
B-1049 Brussels  
Belgium

Dear Commissioner Jourová:

Thank you for your letter regarding our work together to implement the Privacy Shield.

As you noted, our Privacy Shield team is now focused on conducting a robust review of certifications to the Framework submitted by hundreds of organizations. Our team has reviewed and finalized the certifications of more than 500 companies, which now appear on the public Privacy Shield list. Hundreds of additional companies have submitted certifications and are now going through our review process. Our team is pleased with the response to date. The fast pace of the program's growth benefits privacy and is a testament to the need for this critical data transfer mechanism.

Please allow me to address the other implementation issues that you raised in your letter. With regard to the arbitral panel, our teams met in September to continue work on setting up the panel, which includes the U.S. Department of Commerce's upcoming publication of a procurement package related to establishing the arbitral fund. We look forward to continuing to work closely with your team to put in place the procedures and the roster of arbitrators within the six-month time frame.

We also have made important progress to establish procedures to enable Data Protection Authorities (DPAs) to refer cases to us. We have established a dedicated contact to act as a liaison with DPAs, and we have communicated contact information for the DPA liaison to the Article 29 Working Party. We have also developed and shared with the Article 29 Working Party a standard form for DPAs' use to refer complaints regarding an organization's compliance with the Privacy Shield. Our teams recently met with DPAs on the sidelines of their International Conference of Data Protection and Privacy Commissioners to discuss our implementation of the Framework and how we can most effectively coordinate going forward.

With regard to the review process, at this stage, two months after launching the program, as our teams discussed, we believe it is premature to begin planning for an annual review. Instead, we have proposed meeting with DPAs and your team during the DPAs' December

Ms. Věra Jourová  
Page 2

plenary meeting. This would enable close coordination with your team and DPAs as we launch the program on both sides of the Atlantic, and it would help us prepare for the annual review. I understand that DPAs have welcomed our participation during the December meeting, and I hope that this approach will serve as a useful touchpoint for our team and yours.

With regards to the Ombudsperson mechanism, I understand that progress has been made in terms of setting up procedures on the U.S. end, and I refer you to my colleagues at the U.S. Department of State for more details.

I would like to thank you and your team again for the close coordination on and continued dedication to our work on the Privacy Shield. We look forward to continued engagement with you and your team in the weeks and months ahead.

Sincerely,



Penny Pritzker

**From:** [REDACTED]@trade.gov>  
**Sent:** 30 November 2016 03:31  
**To:** [REDACTED] (JUST); [REDACTED] (JUST)  
**Cc:** [REDACTED]  
**Subject:** Privacy Shield arbitration  
**Attachments:** Privacy Shield Statement of Work 11.29.16.docx; ATT00001.htm

**Follow Up Flag:** Follow up  
**Flag Status:** Flagged

Hi [REDACTED]

There is a possibility of some additional changes in this as we finish a legal scrub, but we wanted to share with you.

Happy to talk through the document in a call later this week if you have questions. Let us know.

best,  
[REDACTED]

Sent from my iPhone

**From:** [REDACTED]@trade.gov>  
**Sent:** 09 December 2016 19:48  
**To:** [REDACTED] (JUST); [REDACTED] (JUST)  
**Cc:** [REDACTED]  
**Subject:** FW: Revised SOW  
**Attachments:** Privacy Shield Statement of Work\_12.9.16.docx

**Follow Up Flag:** Follow up  
**Flag Status:** Flagged

Hi [REDACTED]

Good to see you in DC.

Following our meeting, please see the attached arbitration document.

We are aiming to start the process towards publication on Monday, but let us know if you have questions.

Best,  
[REDACTED]

**From:** [REDACTED] (JUST)  
**Sent:** 14 December 2016 15:33  
**To:** [REDACTED]  
**Cc:** [REDACTED]; [REDACTED] (JUST); [REDACTED] (JUST)  
**Subject:** RE: Revised SOW  
**Attachments:** Privacy Shield Statement of Work\_12.9.16.docx

**Follow Up Flag:** Follow up  
**Flag Status:** Flagged

Dear [REDACTED]

Thanks for sending us the draft arbitration document and the changes you introduced following our last meeting in DC.

While these changes already go some way to address our concerns, we would suggest a couple of tweaks – in track changes in the attached document – to make even clearer the point that we will together agree on the rules/fund.

In addition, we think it would be important to ensure that the contractor will have to apply appropriate data protection safeguards for the personal data it receives in the context of arbitration procedures.

Kind regards,  
[REDACTED]

---

**From:** [REDACTED] [m [REDACTED]@trade.gov]  
**Sent:** Friday, December 09, 2016 7:48 PM  
**To:** [REDACTED] (JUST); [REDACTED] (JUST)  
**Cc:** [REDACTED]  
**Subject:** FW: Revised SOW

Hi [REDACTED]

Good to see you in DC.

Following our meeting, please see the attached arbitration document.

We are aiming to start the process towards publication on Monday, but let us know if you have questions.

Best,  
[REDACTED]

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
OFFICE OF GENERAL COUNSEL  
WASHINGTON, DC 20511

DEC 28 2016

Ms. Tiina Astola  
Director-General  
Directorate-General for Justice and Consumers  
European Commission  
Rue Montoyer 59  
1000 Brussels  
BELGIUM

Dear Director General Astola:

I am writing in response to your letter to Kenneth Hyatt of the Department of Commerce, Undersecretary Catherine Novelli, and myself, concerning press reports about alleged foreign intelligence collection activities involving Yahoo! Because of the need to protect sensitive sources and methods, the U.S. Government has a long-established policy that it will neither confirm nor deny particular intelligence activities, and we will not do so in this case.

However, it is important to emphasize that the representations made in my two letters to Justin Antonipillai and Ted Dean of the Department of Commerce, which were incorporated into the Privacy Shield framework, all remain entirely valid. Nothing in the press articles about Yahoo!, if true, is inconsistent with those representations, or would constitute an inappropriate intelligence collection activity or disproportionate interference with individual privacy.

In brief, the articles from Reuters and The New York Times (copies of which are enclosed and from which I am quoting), claim that the alleged activity was "individually approved in an order issued" by a judge of the Foreign Intelligence Surveillance Court, who found probable cause to believe that a certain "digital signature" was "uniquely used by" a "state-sponsored terrorist organization." Thus, any communication that contained that signature would be from that terrorist organization. According to the press reports, the company adapted its existing "system intended to scan emails for child pornography and spam," as well as malware, to search for messages containing that unique signature, and provided the government "a copy of any messages it found that contained the digital signature."


As noted above, we are not in a position to confirm or deny what is reported in these stories. However, if they were true, they would describe foreign intelligence collection that was precisely targeted at important and justified targets, that was judicially authorized in advance, that was conducted pursuant to law, that relied upon a technique that involves no greater intrusion into privacy than the company already engages in by scanning communications for malware, spam or child pornography, and that provided the

Ms. Tiina Astola

Government only communications of a foreign terrorist organization. Thus, nothing in these press reports would in any way cast doubt upon either the representations made in my earlier letters or on the legality of U.S. surveillance activity.

I hope that this information is helpful to you.

Very truly yours,

A handwritten signature in dark ink, appearing to be 'R. Litt', written in a cursive style.

Robert S. Litt

Encl.



Reuters|

Thu Oct 6, 2016 | 10:21pm EDT

## **Yahoo email scan fell under foreign spy law -sources**

By Mark Hosenball and Dustin Volz

(This October 5 story has been corrected to show court order did not come under Section 702 of FISA. Headline and para 1 have also been corrected to remove references to soon-expiring law.)

A Yahoo operation in 2015 to scan the incoming email of its customers for specific information identified by the U.S. government was authorized under a foreign intelligence law, U.S. government officials familiar with the matter said.

Reuters on Tuesday reported that the Yahoo program was in response to a classified U.S. government request to scan emails belonging to hundreds of millions of Yahoo users.

The revelation rekindled a long-running debate in the United States over the proper balance between digital privacy and national security.

The Department of Justice obtained the order from the Foreign Intelligence Surveillance Court, said the sources, who requested anonymity to speak freely.

The order came under the Foreign Intelligence Surveillance Act and related specifically to Yahoo, but it is possible similar such orders have been issued to other telecom and internet companies, the sources said.

Two government sources previously said the request was issued under a provision of the law known as Section 702, but Reuters subsequently learned the information was incorrect. Section 702 will expire on Dec. 31, 2017, unless lawmakers act to renew it.

In a statement on Wednesday, Yahoo said Tuesday's report by Reuters was "misleading" and that the "mail scanning described in the article does not exist on our systems."

When asked to identify any specific way in which the story was misleading, or whether the operation described by Reuters had previously existed, Yahoo declined to comment.

Former Yahoo employees told Reuters that security staff disabled the scan program after they discovered it, and that it had not been reinstalled before Alex Stamos, the company's former top security officer, left the company for Facebook last year.

The intelligence committees of both houses of Congress, which are given oversight of U.S. spy agencies, are now investigating the exact nature of the Yahoo order, sources said.

Privacy advocates expressed alarm at the reported Yahoo program, saying it may amount to an unprecedented use of the authorities granted to the National Security Agency by Congress.

Speaking to students at Georgetown University on Tuesday, former NSA contractor Edward Snowden, who leaked a trove of classified documents to journalists in 2013 exposing NSA surveillance programs, said the Yahoo report renewed questions about whether government surveillance programs are subject to sufficient congressional oversight and public scrutiny.

"That's not to say that this Yahoo program is sinister," Snowden said via satellite. "It could be related to cyber security, where it is related to known malware actors."

Government officials on Wednesday sought to defend U.S. surveillance operations as appropriately balanced and transparent, though they did not deny the Reuters report.

"The United States only uses signals intelligence for national security purposes, and not for the purpose of indiscriminately reviewing the emails or phone calls of ordinary people," Richard Kolko, a spokesman for the U.S. Office of the Director of National Intelligence, said in a statement.

White House spokesman Josh Earnest told reporters Tuesday that he could not confirm the existence of specific intelligence programs or intelligence tools, but defended the checks and balances placed on what information or methods the intelligence community can seek.

(Reporting by Mark Hosenball and Dustin Volz in Washington Additional reporting by Joseph Menn in San Francisco; Editing by Jonathan Weber and Grant McCool)

*New York Times*

*Yahoo Said to Have Aided U.S. Email Surveillance by  
Adapting Spam Filter*

By CHARLIE SAVAGE and NICOLE PERLROTH OCT. 5, 2016

A system intended to scan emails for child pornography and spam helped Yahoo satisfy a secret court order requiring it to search for messages containing a computer “signature” tied to the communications of a state-sponsored terrorist organization, several people familiar with the matter said on Wednesday.

Two government officials who spoke on the condition of anonymity said the Justice Department obtained an individualized order from a judge of the Foreign Intelligence Surveillance Court last year. Yahoo was barred from disclosing the matter.

To comply, Yahoo customized an existing scanning system for all incoming email traffic, which also looks for malware, according to one of the officials and to a third person familiar with Yahoo’s response, who also spoke on the condition of anonymity.

With some modifications, the system stored and made available to the Federal Bureau of Investigation a copy of any messages it found that contained the digital signature. The collection is no longer taking place, those two people said.

The order was unusual because it involved the systematic scanning of all Yahoo users’ emails rather than individual accounts; several other tech companies said they had not encountered such a demand.

News of the order has opened a new chapter in a public debate over the trade-offs between security needs and privacy rights that has cast a spotlight on the sometimes cooperative, sometimes antagonistic relationship between Silicon Valley companies and the United States government.

It comes six months after a standoff between the F.B.I. and Apple, in which the government obtained a federal magistrate’s order to force the company to help it unlock an encrypted iPhone from one of the attackers in the December mass shooting in San Bernardino, Calif. The F.B.I. gave up the fight with Apple after it found a way into the iPhone without the company’s help.

By contrast, Yahoo cooperated with the Foreign Intelligence Surveillance Court order, although the technical burden on the company appears to have been significantly lighter than the one the F.B.I. placed on Apple.

Details of Yahoo’s cooperation with the court order come two weeks after the company reported that hackers had broken into its computer network, stealing the credentials of 500 million users. Yahoo engineers discovered the breach this summer, two years after it

had occurred, and just weeks after Verizon Communications announced plans to buy the troubled internet company for \$4.8 billion.

The two government officials familiar with the matter said the digital signature Yahoo was ordered to look for last year was individually approved in an order issued by a judge, who was persuaded that there was probable cause to believe that it was uniquely used by a foreign power.

Investigators had learned that agents of the foreign terrorist organization were communicating using Yahoo's email service and with a method that involved a "highly unique" identifier or signature, but the investigators did not know which specific email accounts those agents were using, the officials said.

The officials' description of the unusual surveillance operation carried out at Yahoo shed new light on a report by Reuters that has attracted widespread attention and provoked outrage among privacy and technology specialists.

The Reuters article reported that in response to a "broad demand" from the government, Yahoo had "secretly built a custom software program to search all of its customers' incoming emails for specific information provided by U.S. intelligence officials."

According to the government officials, Yahoo was served with an individualized court order to look only for code uniquely used by the foreign terrorist organization. Two sources, including one of the officials, portrayed it as adapting the scanning systems that it already had in place to comply with that order rather than building a brand-new capability. The other official did not comment on the technology. The officials did not name the terrorist organization.

Asked on Wednesday about the information obtained by The New York Times, Suzanne Phillion, a Yahoo spokeswoman, said the company had nothing further to say. Earlier in the day, the company said in a statement that the Reuters article was "misleading."

"We narrowly interpret every government request for user data to minimize disclosure," the Yahoo statement said. "The mail scanning described in the article does not exist on our systems."

Richard Kolko, a spokesman for the Office of the Director of National Intelligence, declined in a statement to discuss specific foreign intelligence collection techniques, but referred to the Foreign Intelligence Surveillance Act, or FISA.

"Under FISA, activity is narrowly focused on specific foreign intelligence targets and does not involve bulk collection or use generic key words or phrases," he said. "The United States only uses signals intelligence for national security purposes, and not for the purpose of indiscriminately reviewing the emails or phone calls of ordinary people."

Technology companies like Yahoo, Google and Microsoft scan for child pornography and are required to report any discoveries to the National Center for Missing and Exploited Children. They similarly search traffic for malware and spam, which companies disclose in their terms of service.

There is no engineering limitation preventing technology companies from using their spam and child pornography filtering systems to search email traffic for other sorts of digital signatures, said Hany Farid, chairman of the computer science department at Dartmouth, who helped develop the child pornography scanning system with Microsoft.

But the use of that technology to carry out an order from the Foreign Intelligence Surveillance Court to search for a digital signature used by a foreign power is rare, and one of the officials portrayed it as innovative.

"This is another example of how the government is pushing secretly novel or innovative interpretations of surveillance law" to conduct wiretapping in broader ways than the public realizes, said Jennifer Granick, the director of civil liberties at the Stanford Law School Center for Internet and Society.

The government has not released any intelligence court opinion explaining how the judge interpreted FISA to authorize such surveillance. Although Congress in June 2015 enacted a law that required the government to make public novel and significant rulings by the court, the order to Yahoo appears to have predated that legislation, the USA Freedom Act, by several months.

Yahoo has an inconsistent record with meeting government data demands. In 2007, the company settled a lawsuit related to allegations that it helped the Chinese government crack down on journalists by passing along their Yahoo emails.

But that year, the firm fought a legal battle, then secret, before the Foreign Intelligence Surveillance Court, challenging a mandate that it turn over, without a warrant, emails from user accounts the F.B.I. and the National Security Agency said belonged to noncitizens abroad who had been targeted for surveillance.

That litigation became an important test of whether Congress could legalize the Bush administration's warrantless surveillance program through the Protect America Act and, later, the FISA Amendments Act. Ultimately, the intelligence court ruled against Yahoo, and after being threatened with a huge fine, the company cooperated.

Yahoo was not able to clarify details of the Reuters article on Tuesday because orders from the Foreign Intelligence Surveillance Court are secret by law, and an increasing number of other government requests come with gag orders that prohibit tech companies from even acknowledging they exist.

Tech companies complain that such gag orders make it impossible for them to explain to customers what sort of data they do and do not turn over. Twitter and Microsoft have

separately sued the Justice Department over the gag order practice, and both cases are pending.

Dozens of other companies have filed briefs in support of Microsoft. In its brief, Apple said it had received about 590 gag orders, of unlimited or indefinite durations, in the first eight months of 2016.

Vindu Goel contributed reporting.

**From:** [REDACTED]@trade.gov>  
**Sent:** 18 January 2017 20:52  
**To:** [REDACTED] (JUST); [REDACTED] (JUST)  
**Cc:** [REDACTED]  
**Subject:** PS Arbitration fact sheet and Statement of Work  
**Attachments:** Factsheet--arbitration mechanism 1.17.docx; Privacy Shield Statement of Work\_12.21.16.docx

**Follow Up Flag:** Follow up  
**Flag Status:** Flagged

Hi [REDACTED]

Attached is the fact sheet we propose to publish on our website regarding the arbitration mechanism procurement. We would like to publish this tomorrow and welcome any comments.

Also, for your reference, I have attached the final statement of work.

Please let us know if you have time to talk tomorrow before 3:00 DC time.

Thanks!

[REDACTED]

[REDACTED]

U.S. Department of Commerce

[REDACTED]

**From:** [REDACTED]@trade.gov>  
**Sent:** 24 January 2017 20:24  
**To:** [REDACTED] (JUST); [REDACTED] (JUST)  
**Cc:** [REDACTED]  
**Subject:** arbitration post on PS website

**Follow Up Flag:** Follow up  
**Flag Status:** Flagged

Hi [REDACTED]

This is just to let you know that our post about the arbitration mechanism is up:

<https://www.privacyshield.gov/Arbitration-Fact-Sheet>

Thanks!

[REDACTED]

[REDACTED]

U.S. Department of Commerce

[REDACTED]



**From:** [REDACTED]@trade.gov>  
**Sent:** 18 February 2017 00:42  
**To:** [REDACTED] (JUST)  
**Cc:** [REDACTED] (JUST); [REDACTED] (JUST)  
**Subject:** RE: arbitration post on PS website  
**Attachments:** Privacy Shield Arbitral Panel 2.17.docx

**Follow Up Flag:** Follow up  
**Flag Status:** Flagged

Hi [REDACTED]

I hope you are well. I'm sorry we didn't connect this week, and I will be in Vietnam next week at APEC meetings. In an effort to keep things moving, attached is a draft public notice that we propose to use to recruit arbitrators for the PS arbitral list. We welcome your thoughts and if it makes sense, we can aim for a call to discuss this the week after next if that is convenient for you.

I look forward to hearing from you.

All the best,

[REDACTED]  
[REDACTED]  
[REDACTED]  
U.S. Department of Commerce  
[REDACTED]  
[REDACTED]

---

**From:** [REDACTED]@ec.europa.eu [REDACTED]@ec.europa.eu  
**Sent:** Monday, February 13, 2017 1:33 PM  
**To:** [REDACTED]  
**Cc:** [REDACTED]@ec.europa.eu; [REDACTED]@ec.europa.eu  
**Subject:** RE: arbitration post on PS website

Hi [REDACTED]

I hope this email finds you well.

Any news on the arbitration front (e.g. draft notice for selection of arbitrators)?

Should we schedule a conference call in the coming days?

Many thanks.

Best,

[REDACTED]

**From:** [REDACTED]@trade.gov]  
**Sent:** Tuesday, January 24, 2017 8:24 PM  
**To:** [REDACTED] (JUST); [REDACTED] (JUST)  
**Cc:** [REDACTED]  
**Subject:** arbitration post on PS website

Hi [REDACTED]

This is just to let you know that our post about the arbitration mechanism is up:

<https://www.privacyshield.gov/Arbitration-Fact-Sheet>

Thanks!

[REDACTED]

[REDACTED]

U.S. Department of Commerce

[REDACTED]

(2017) 2123233



U. S. Department of Justice

Washington, D.C. 20530

February 22, 2017

Tiina Astola  
Director General, Justice and Consumers  
European Commission, Directorate for Justice and Consumers  
Montoyer 59  
Bruxelles, Belgium 1040

Re Executive Order "Enhancing Public Safety in the Interior of the United States"

Dear Ms Astola:

Thank you for your letter of February 7, 2017, concerning Section 14 of the President's January 25, 2017 Executive Order, entitled "Enhancing Public Safety in the Interior of the United States." Your letter seeks further clarification regarding the possible effect of Section 14 on transfers of personal data under the EU-U.S. Privacy Shield ("Privacy Shield") and the U.S.-EU Data Privacy and Protection Agreement ("DPPA").

As you know, the United States has implemented the DPPA by enacting the Judicial Redress Act of 2015. Section 14 of the Executive Order does not affect the privacy rights extended by the Judicial Redress Act to Europeans. Nor does Section 14 affect the commitments the United States has made under the DPPA or the Privacy Shield.

The United States Government looks forward to working closely with the Commission in the weeks and months ahead to protect the privacy and the security of citizens of the United States and the European Union.

Sincerely,

A handwritten signature in dark ink, appearing to read "B. Swartz", written over a horizontal line.

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

**From:** [REDACTED] (JUST)  
**Sent:** 27 February 2017 21:21  
**To:** [REDACTED]  
**Cc:** [REDACTED] (JUST); [REDACTED] (JUST)  
**Subject:** RE: arbitration post on PS website  
**Attachments:** Privacy Shield Arbitral Panel 2.17.docx

**Follow Up Flag:** Follow up  
**Flag Status:** Flagged

Dear [REDACTED]

As promised, please find attached some comments/questions on the draft public notice.

Happy to discuss over the phone.

Best regards,  
[REDACTED]

PS: if you would have a name for the "acting Ombudsperson", that would be great (we have received some questions from both members of parliament and our DPAs)

---

**From:** [REDACTED]@trade.gov]  
**Sent:** Saturday, February 18, 2017 12:42 AM  
**To:** [REDACTED] (JUST)  
**Cc:** [REDACTED] (JUST); [REDACTED] (JUST)  
**Subject:** RE: arbitration post on PS website

[REDACTED]

I hope you are well. I'm sorry we didn't connect this week, and I will be in Vietnam next week at APEC meetings. In an effort to keep things moving, attached is a draft public notice that we propose to use to recruit arbitrators for the PS arbitral list. We welcome your thoughts and if it makes sense, we can aim for a call to discuss this the week after next if that is convenient for you.

I look forward to hearing from you.

All the best,

[REDACTED]

[REDACTED]

U.S. Department of Commerce  
[REDACTED]

**From:** [REDACTED] [REDACTED]@ec.europa.eu [REDACTED]@ec.europa.eu  
**Sent:** Monday, February 13, 2017 1:33 PM  
**To:** [REDACTED]  
**Cc:** [REDACTED]@ec.europa.eu; [REDACTED]@ec.europa.eu  
**Subject:** RE: arbitration post on PS website

Hi [REDACTED]

I hope this email finds you well.

Any news on the arbitration front (e.g. draft notice for selection of arbitrators)?

Should we schedule a conference call in the coming days?

Many thanks.

Best,  
[REDACTED]

---

**From:** [REDACTED]@trade.gov]  
**Sent:** Tuesday, January 24, 2017 8:24 PM  
**To:** [REDACTED] (JUST); [REDACTED] (JUST)  
**Cc:** [REDACTED]  
**Subject:** arbitration post on PS website

Hi [REDACTED]

This is just to let you know that our post about the arbitration mechanism is up:

<https://www.privacyshield.gov/Arbitration-Fact-Sheet>

Thanks!

[REDACTED]

[REDACTED]

U.S. Department of Commerce  
[REDACTED]

**From:** [REDACTED]@trade.gov>  
**Sent:** 01 March 2017 21:53  
**To:** [REDACTED] (JUST)  
**Cc:** [REDACTED] (JUST); [REDACTED] (JUST)  
**Subject:** RE: arbitration post on PS website

**Follow Up Flag:** Follow up  
**Flag Status:** Flagged

Hi [REDACTED]

Thank you for your comments on the public notice regarding the recruitment of panelists. We are reviewing your comments now and will respond separately.

On a related note, I want to update you on the procurement process for selecting a contractor to manage the arbitral fund and serve as the arbitration administrator. [REDACTED]

[REDACTED] we published a full and open solicitation, available at:

[https://www.fbo.gov/index?s=opportunity&mode=form&id=7ec7c3a3e8cd7768ef2e8b686adcf3bd&tab=core&\\_cview=0](https://www.fbo.gov/index?s=opportunity&mode=form&id=7ec7c3a3e8cd7768ef2e8b686adcf3bd&tab=core&_cview=0). This solicitation is open until March 10. [REDACTED]

To your question on the ombudsperson, Judy Garber is unofficially acting as the Under Secretary and filling this role on an informal basis while State waits for new officials to be nominated and confirmed.

I also wanted to ensure you knew that [REDACTED] from our team, [REDACTED] from the FTC, and [REDACTED] at USEU are planning to participate in a meeting of the Article 29 Working Party's Expert Subgroup on International Transfers on March 14 to discuss our implementation work and address more detailed questions at the staff level, as contemplated back in December. We assume that someone from the Commission also participates, but weren't sure. [REDACTED] inquired if you or [REDACTED] would be interested in touching base briefly ahead of that, perhaps over coffee. I believe they are available late afternoon on the 13<sup>th</sup> or before the meeting on the 14<sup>th</sup>.

Finally, you may have heard that our new Secretary was confirmed yesterday and is now in office. You will be pleased to learn that in his very first address this morning, Secretary Ross confirmed his commitment to the Privacy Shield program. Below is an article about this from earlier today.

I will be in touch shortly on the FRN. Thanks again!

## **Trump's new Commerce secretary throws his weight behind Privacy Shield**

By Nancy Scola

03/01/2017 10:25 AM EDT

Newly confirmed Commerce Secretary Wilbur Ross signaled his support for a transatlantic data transfer agreement whose fate is being closely watched by both the U.S. tech industry and European privacy advocates, telling agency employees today that "we must build upon the hard work many of you have done in support of Privacy Shield."

That deal, which offers citizens of European Union countries added protections when it comes to the security of their personal data transferred to the United States, was hammered out by Obama administration officials and signed in July. It replaced a previous 16-year-old agreement between the U.S. and Europe that had fallen apart as the result of a case brought by an Austrian privacy activist over Facebook's handling of data.

Some in Europe, though, have raised questions about whether the last administration's assurances will hold up under President Donald Trump, particularly in light of a Trump immigration executive order that instructed agencies to exclude foreigners from privacy protections.

Ross was confirmed late Tuesday and addressed agency employees this morning at the Commerce Department's headquarters in Washington.

*To view online:*

<https://www.politicopro.com/tech/whiteboard/2017/03/trumps-new-commerce-secretary-throws-his-weight-behind-privacy-shield-084287>

[REDACTED]  
[REDACTED]  
[REDACTED]  
U.S. Department of Commerce  
[REDACTED]  
[REDACTED]

---

**From:** [REDACTED]@ec.europa.eu [REDACTED]@ec.europa.eu]  
**Sent:** Monday, February 27, 2017 2:41 AM  
**To:** [REDACTED]  
**Cc:** [REDACTED]@ec.europa.eu; [REDACTED]@ec.europa.eu  
**Subject:** RE: arbitration post on PS website

Dear [REDACTED]

Just to say that we have some comments but did not manage on Friday to discuss internally – we will come back to you on this today.

On a different topic: could you let us know who is currently "acting" as Ombudsperson in the State Department (we could see from the SD's webpage that so far the post of C. Novelli as Under Secretary has not yet been filled)?

Best regards,

[REDACTED]

**From:** [REDACTED] (JUST)  
**Sent:** Thursday, February 23, 2017 9:09 PM  
**To:** [REDACTED]  
**Cc:** [REDACTED] (JUST); [REDACTED] (JUST)  
**Subject:** RE: arbitration post on PS website

Dear [REDACTED]

Many thanks for sending us the draft public notice.

We had a first look and will come back to you tomorrow with any comments.

Best regards,

[REDACTED]

**From:** [REDACTED]@trade.gov]  
**Sent:** Saturday, February 18, 2017 12:42 AM  
**To:** [REDACTED] (JUST)  
**Cc:** [REDACTED] (JUST); [REDACTED] (JUST)  
**Subject:** RE: arbitration post on PS website

Hi [REDACTED]

I hope you are well. I'm sorry we didn't connect this week, and I will be in Vietnam next week at APEC meetings. In an effort to keep things moving, attached is a draft public notice that we propose to use to recruit arbitrators for the PS arbitral list. We welcome your thoughts and if it makes sense, we can aim for a call to discuss this the week after next if that is convenient for you.

I look forward to hearing from you.

All the best,

[REDACTED]

[REDACTED]

U.S. Department of Commerce

[REDACTED]



[REDACTED]

---

**From:** [REDACTED]@ec.europa.eu ([REDACTED]@ec.europa.eu)  
**Sent:** Monday, February 13, 2017 1:33 PM  
**To:** [REDACTED]  
**Cc:** [REDACTED]@ec.europa.eu; [REDACTED]@ec.europa.eu  
**Subject:** RE: arbitration post on PS website

Hi [REDACTED]

I hope this email finds you well.

Any news on the arbitration front (e.g. draft notice for selection of arbitrators)?

Should we schedule a conference call in the coming days?

Many thanks.

Best,

[REDACTED]

---

**From:** [REDACTED]@trade.gov  
**Sent:** Tuesday, January 24, 2017 8:24 PM  
**To:** [REDACTED] (JUST); [REDACTED] (JUST)  
**Cc:** [REDACTED]  
**Subject:** arbitration post on PS website

Hi [REDACTED]

This is just to let you know that our post about the arbitration mechanism is up:

<https://www.privacyshield.gov/Arbitration-Fact-Sheet>

Thanks!

[REDACTED]

[REDACTED]

U.S. Department of Commerce

[REDACTED]

AREJ (2017) 2430913

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
OFFICE OF GENERAL COUNSEL  
WASHINGTON, DC 20511

April 3, 2017

Ms. Tiina Astola  
Director-General  
Directorate-General for Justice and Consumers  
European Commission  
Rue Montoyer 59  
1000 Brussels  
BELGIUM

Dear Director-General Astola:

I am writing in response to your 2 March 2017 letter concerning, among other things, media reports about alleged foreign intelligence collection activities involving Yahoo! As Mr. Litt stressed in his 28 December 2016 letter, because of the need to protect sensitive sources and methods, the U.S. Government has a long-established policy that it will neither confirm nor deny particular intelligence activities. Accordingly, I am not in a position to elaborate on Mr. Litt's response to you but wish to underscore the fact that, even if true, nothing in the press articles about Yahoo! is inconsistent with the representations he made in his 22 February and 21 June 2016 letters or would constitute an inappropriate intelligence collection activity or disproportionate interference with individual privacy.

You have separately asked about the status of the Privacy and Civil Liberties Oversight Board. The Board is a permanent independent agency of the Executive Branch and, although the Board's Membership is changing, it continues to perform its important oversight work in furtherance of its mandate through the remaining Board Member and a permanent professional staff.

Finally, you have asked for additional information on the new procedures to allow for sharing of certain signals intelligence information. In early January of this year, the Director of National Intelligence, in coordination with the Secretary of Defense and with the approval of the Attorney General, issued the "Procedures for the Availability or Dissemination of Raw Signals Intelligence Information by the National Security Agency under Section 2.3 of Executive Order 12333." These procedures,<sup>1</sup> along with additional explanatory information,<sup>2</sup> are publicly available and were posted on IC on the Record (<https://icontherecord.tumblr.com>). Such publication was made in line with the *Principles of Intelligence Transparency for the*

<sup>1</sup> The procedures can be found here: <https://tumblr.co/ZZQjsq2H4R8Kh>

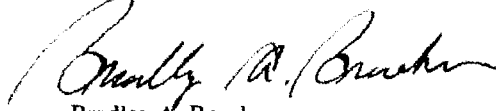
<sup>2</sup> Additional explanatory information can be found here: <https://tumblr.co/ZZQjsq2H4QILY>

Ms. Tiina Astola

*Intelligence Community.*<sup>3</sup> The procedures are designed to enable authorized Intelligence Community (IC) elements to bring to bear their own analytic expertise to reviewing signals intelligence in support of their missions. Before gaining access to raw signals intelligence, IC elements must satisfy a set of specific requirements. For example, they must justify their need to access raw signals intelligence, implement rigorous privacy rules that are based on those that NSA follows, and put in place strict oversight and compliance measures that are comparable to those employed by NSA. It is also important to highlight that the procedures emphasize that any information shared pursuant to these procedures is also subject to the protections of Presidential Policy Directive No. 28 and agency implementing procedures.

I hope this information is useful to you and the Commission.

Sincerely,

A handwritten signature in black ink, appearing to read "Bradley A. Brooker". The signature is fluid and cursive, with the first name "Bradley" being more prominent.

Bradley A. Brooker  
General Counsel (Acting)

---

<sup>3</sup> The Principles of Intelligence Transparency and related materials can be found here:  
<https://www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles>

Brussels, 29 February 2016  
Ares(2016)

Dear Mr Moraes,

I hereby wish to personally transmit to you a new Commission Communication to the European Parliament and the Council on *"Transatlantic Data Flows: Restoring Trust through Strong Safeguards"*, adopted by the Commission today, as well as the draft adequacy decision on the EU – U.S. Privacy Shield.

The Commission Communication takes stock of how far we have come in fulfilling the objectives formulated in our Communication of November 2013<sup>1</sup>. I greatly value the cooperation with your committee throughout these years, which has allowed us to achieve significant improvements in the protection of personal data of EU citizens, through the conclusion of the EU data protection reform, as well as robust new arrangements with the U.S..

In particular, we have achieved an important change in U.S. legislation through the adoption of the Judicial Redress Act, which was signed into law by President Obama on 24 February. The effective enjoyment of these rights by our citizens is subject to the ratification of the EU-US Data Protection "Umbrella" Agreement. As this is an international agreement, the Commission will shortly propose to the Council to adopt the decision enabling the signature of the agreement and thereafter the text will be submitted to the European Parliament for its consent on the conclusion of the agreement. The Commission continues to be available for any clarifications, which would allow Members to make an informed assessment of the agreement.

As regards the EU-U.S. Privacy Shield, the enclosed package includes all the documents from the United States government pertaining to the new arrangement. They contain the binding commitments, representations and assurances, which, together with the overall US legal framework, allow the Commission to propose an adequacy decision regarding the EU-US Privacy Shield.

Mr Claude Moraes, MEP  
Chair of the Committee on Civil Liberties, Justice and Home Affairs  
Email: [claudio.moraes@europarl.europa.eu](mailto:claudio.moraes@europarl.europa.eu)

---

<sup>1</sup> Communication from the Commission to the European Parliament and the Council: Rebuilding Trust in EU-US Data Flows, COM(2013) 846final of 27.11.2013.

The draft decision will now be sent to the "Article 29 Working Party" (comprising the EU DPAs) for an opinion and then go through the comitology procedure before it can be adopted by the European Commission, as an implementing measure. Unlike the Umbrella Agreement, the EU-U.S. Privacy Shield is not an international agreement and will therefore not be submitted to the European Parliament for its consent. Nevertheless, we stand ready to provide to the European Parliament and your committee any information and explanations that would be useful on this new framework. In particular, we are at your disposal to provide technical explanations ahead of the hearing your committee plans for mid-March.

Once adopted, the Commission shall continuously monitor the implementation of the decision, including through annual joint reviews and shall report the findings to the European Parliament and Council. Should there be shortcomings in the application of the framework, the Commission shall activate the possibility to suspend the decision the EU-U.S. Privacy Shield and withdraw the benefits of the adequacy finding.

Finally, I would like to highlight that today's Communication calls for further reforms of U.S. intelligence programmes, as well as calling on the U.S. to continue to pursue efforts towards a comprehensive system of privacy and data protection. The Commission will follow these matters closely. Given the essential role of the U.S. Congress in any further reforms, I would greatly welcome continued efforts by Members of your Committee to engage with legislators on the other side of the Atlantic to that end.

I look forward to our continuing cooperation.

Yours sincerely,

Věra Jourová

Brussels, 29 February 2016  
Ares(2016)

Dear Mr van der Steur,

I have the pleasure of sending you attached the draft adequacy decision on the EU – U.S. Privacy Shield, as well as a new Commission Communication on *"Transatlantic Data Flows: Restoring Trust through Strong Safeguards"*, adopted by the Commission today.

The EU-U.S Privacy Shield package includes all the documents from the United States government pertaining to the new arrangement. They contain the binding commitments, representations and assurances, which, together with the overall US legal framework, allow the Commission to propose an adequacy decision regarding the EU-US Privacy Shield.

The draft decision will now be sent to the "Article 29 Working Party" (comprising the EU DPAs) for an opinion and then go through the comitology procedure (vote by Member State experts) before it can be adopted by the European Commission, as an implementing measure, under Directive 95/46/EC.

Today, the Commission has also adopted a Communication on Transatlantic Data Flows, which takes stock of how far we have come in fulfilling the objectives formulated in our Communication of November 2013<sup>1</sup>. We have made significant improvements in the protection of personal data of EU citizens, through the conclusion of the EU data protection reform as well as robust new arrangements with the U.S.. Your Presidency now has unique opportunity to finalise these processes.

In particular, we have achieved an important change in the US legislation by the adoption of the Judicial Redress Act, which was signed into law by President Obama on 24 February. The effective enjoyment of these rights by our citizens is subject to the ratification by the EU of the EU-US "Umbrella" Agreement. As this is an international agreement, the Commission will shortly propose to the Council to adopt the decision enabling the signature of the agreement, which we hope could take place at the EU-US Ministerial Meeting in Amsterdam on 2<sup>nd</sup> of June. Once this first step is accomplished, the agreement will be submitted to the European Parliament for its consent.

Mr. Ard van der Steur  
Minister of Security and Justice

---

<sup>1</sup> Communication from the Commission to the European Parliament and the Council: Rebuilding Trust in EU-US Data Flows, COM(2013) 846 final of 27.11.2013.

I look forward to our continuing cooperation and we remain available for clarifications that the Presidency or the Council may require. In particular, I look forward to informing Justice Ministers of the state of play at the upcoming Justice and Home Affairs Council on 10-11 March.

Yours sincerely,

A solid black rectangular box used to redact the signature of Věra Jourová.

Věra Jourová

**VĚRA JOUROVÁ**  
*Member of the European Commission*

Brussels, 29 February 2016  
Ares(2016)

Dear Ms Falque-Pierrotin,

I hereby wish to personally transmit to you the draft adequacy decision on the EU – U.S. Privacy Shield, as well as a new Commission Communication on Transatlantic Data Flows adopted today.

As called for in the statement of the Article 29 Working party of 3 February, the enclosed package includes all the documents from the United States government pertaining to the new arrangement. They contain the binding commitments, representations and assurances, which, together with the overall U.S. legal framework, allow the Commission to propose an adequacy decision regarding the EU-U.S. Privacy Shield.

As I stated before your Working Party on 3 February, I am convinced that we have obtained important and unprecedented commitments from the U.S. under the EU-U.S. Privacy Shield. The new arrangement represents an opportunity to enshrine the recent and ongoing U.S. surveillance reforms in a transatlantic context and to continue closely monitoring them in the future annual joint reviews.

Let me also add that, following my exchange with the Working Party on 3 February, we have been able to secure with the U.S. that the new redress mechanism for national security issues ("Ombudsperson") will also be available to EU data subjects where data has been transferred to the U.S. under other transfer tools, such as contractual clauses, binding corporate rules or derogations. This was a key point raised by several authorities in our meeting.

The Commission now looks forward to receiving the opinion of the Article 29 Working Party, pursuant to Article 30(1)(b) of Directive 95/46/EC. We stand ready to provide you and the Working Party with any information and explanations that you may require in this context. Following the receipt of your opinion, the next step in the procedure is a decision of the Member States in comitology.

Isabelle Falque-Pierrotin  
Chair of the Article 29 Working Party  
The Secretariat of Article 29 Working Party  
rue Montoyer, 59, Office 02/37  
B-1049 Brussels, Belgium



In particular, we have achieved an important change in the US legislation through the adoption of the Judicial Redress Act, which was signed into law by President Obama on 24 February. The effective enjoyment of these rights by our citizens is subject to the ratification of the EU-US Data Protection "Umbrella" Agreement. As this is an international agreement, the Commission will shortly propose to the Council to adopt the decision enabling the signature of the agreement and thereafter the text will be submitted to the European Parliament for its consent.

Yours sincerely,

\_\_\_\_\_

<sup>1</sup> Communication from the Commission to the European Parliament and the Council: Rebuilding Trust in EU-US Data Flows, COM(2013) 846 final of 27 June 2013, (validity of electronic documents) of Commission Decision 2004/563.



EUROPEAN COMMISSION  
DIRECTORATE-GENERAL JUSTICE AND CONSUMERS

Director-General

Brussels, 11/03/2016  
DG JUST/TA/Ares(2016)

Mr. Giovanni Butarelli  
European Data Protection  
Supervisor  
Rue Montoyer 30  
Brussels

Dear Mr Butarelli,

I hereby wish to send to you the draft adequacy decision on the EU – U.S. Privacy Shield, as well as a new Commission Communication on *"Transatlantic Data Flows: Restoring Trust through Strong Safeguards"*.

The enclosed package includes all the documents from the United States government pertaining to the new arrangement. They contain the binding commitments, representations and assurances, which, together with the overall U.S. legal framework, allow the Commission to propose an adequacy decision regarding the EU-US Privacy Shield.

The draft decision is being sent to the Article 29 Working Party for its opinion pursuant to Article 30(1)(b) of Directive 95/46/EC.

We would like to consult you on this draft decision and look forward to receiving your opinion. The draft decision would then go through the comitology procedure before it can be adopted by the European Commission, as an implementing measure, under Directive 95/46/EC.

The Commission Communication takes stock of how far we have come in fulfilling the objectives formulated in our Communication of November 2013<sup>1</sup>. We have made significant improvements in the protection of personal data of EU citizens, through the conclusion of the EU data protection reform as well as the draft agreements with the US. In particular, we have achieved an important change in the U.S. legislation by the adoption of the Judicial Redress Act which was signed into law by President Obama on February 19, 2015. The Act provides for a new mechanism by which EU citizens can seek redress in U.S. courts for data breaches by U.S. companies subject to the Act.

As this is an international agreement, the Commission will soon propose to the Council to adopt the decision enabling the signature of the agreement. Thereafter, the agreement will be submitted to the European Parliament for its consent.

I look forward to hearing from you.

Yours sincerely,

A large black rectangular box redacting the signature of Tuna ASTOLA.

Tuna ASTOLA

**VĚRA JOUROVÁ**  
*Member of the European Commission*

Brussels,  
Ares(2016)

Dear Ms O'Reilly,

I refer to your letter of 22 February 2016 on the use of the term 'ombudsperson' for the new complaint-handling office created under the recently concluded EU-U.S. Privacy Shield.

Since we received your letter, the full documentation of this arrangement has been made available on our website.<sup>1</sup> I trust that you have already had the opportunity to examine the texts, in particular Annex III of the Commission's draft adequacy decision containing the details of the newly established "EU-U.S. Privacy Shield Ombudsperson Mechanism Regarding Signals Intelligence." You will see that this mechanism contains a number of important features that we believe should address the concerns you expressed in your letter.

In particular, I would like to highlight the following salient elements of this mechanism:

Firstly, the U.S. government will establish a new complaint-handling position within the Department of State, that will be occupied by a high-ranking official, Under Secretary of State Catherine Novelli. The new office, which the US government has termed "Ombudsperson", shall ensure that individual enquiries and complaints relating to the potential access by U.S. intelligence authorities to data transmitted from the EU to the United States will be properly investigated and receive a timely response. This constitutes major progress from the current situation where U.S. rules (Presidential Policy Directive 28) only foresees a contact person for foreign governments that wish to raise concerns regarding U.S. signals intelligence activities. At the same time, individuals will be able to address their complaint, in their own language, to the Member States bodies competent for the oversight of national security services and eventually to a centralised EU individual complaint handling body. These bodies will then interface, on behalf of the individual, with the Ombudsperson, thereby easing the burden on individuals in the exercise of their fundamental rights.

Ms Emily O'Reilly  
European Ombudsman

---

<sup>1</sup> See: [http://europa.eu/rapid/press-release\\_IP-16-433\\_en.htm](http://europa.eu/rapid/press-release_IP-16-433_en.htm) and [http://europa.eu/rapid/press-release\\_MEMO-16-434\\_en.htm](http://europa.eu/rapid/press-release_MEMO-16-434_en.htm)

Secondly, there is a clear commitment from the U.S. government that the Ombudsperson will have to come back to the complainant with a timely response, confirming that the complaint has been thoroughly investigated and that either U.S. law has been complied with or, in cases of non-compliance, that this situation has been remedied. This is a very important element, given that such confirmation necessarily presupposes that the Ombudsperson will have to receive relevant and sufficient information allowing her to make an own assessment, both as regards the investigation carried out and the compliance of the respective national intelligence activities with U.S. law.

Third, the Ombudsperson will be independent from the U.S. intelligence community. While she will act under the authority of the Secretary of State, the latter is bound by the relevant commitments made to the Commission, including as to the timely response to be given to EU individuals. Moreover, the Ombudsperson should not be viewed in isolation: in performing her responsibilities to ensure an appropriate response to and resolution of complaints, the Ombudsperson will closely coordinate with a number of oversight bodies that are themselves independent from the intelligence agencies whose conduct will be investigated. This concerns, in particular, the statutorily independent Inspectors-General that have been created for the various elements of the Intelligence Community and that have broad powers to conduct investigations, audits and reviews of intelligence programmes; the various Civil Liberties and Privacy Officers in those authorities; and the Privacy and Civil Liberties Oversight Board (PCLOB), an independent agency within the executive branch charged with protecting privacy and civil liberties in the field of counterterrorism policies. In this regard, and with a view to democratic accountability, it is important to know that these bodies report on their findings directly to Congress, thereby allowing the latter to exercise its oversight function. Together with them, the Ombudsperson will be able to guarantee independent oversight of the U.S. intelligence community.

Fourth, the European Commission will continuously monitor the overall functioning of the Privacy Shield framework to ensure it is complied with and still meets the adequacy requirements set out by the Court of Justice. Together with the U.S. authorities, it will carry out an Annual Joint Review of the implementation of the Privacy Shield arrangement which will also involve the participation of the Ombudsperson as necessary. The Commission will use this opportunity to check whether the Ombudsperson mechanism operates properly and in particular delivers timely responses as required. Should this not be the case, this could trigger the suspension of the adequacy decision, as is made clear in our draft decision.

Finally, I would like to draw your attention to the fact that the new Ombudsperson function will be a comprehensive mechanism covering complaints from any EU individual for all personal data transferred to the U.S. irrespective of the means of transfer (whether transferred under the Privacy Shield, standard contractual clauses or binding corporate rules, or any of the derogations permitted under the present or future data protection acquis). In other words, no distinction is made either as regards the individual who can make a complaint or the method of transfer of his or her personal data.

The Commission appreciates that this particular mechanism may differ in a number of aspects from an Ombudsman as defined by the International Ombudsman Institute. This is explained by the specific purposes of the mechanism, and the particularly sensitive context of national security. This notwithstanding, the Commission believes that the mechanism will play an important role in safeguarding the rights of EU individuals where their personal data have been transferred to the United States.

I trust that these explanations are helpful to you.

Yours sincerely,

A large black rectangular box redacting the signature of Věra Jourová.

Věra Jourová



European Parliament

Committee on Civil Liberties, Justice and Home Affairs  
The Chairman

IPOL-COM-LIBE D (2016) 30855

D 312451 28.06.2016

**Ms Věra JOUROVÁ**  
Commissioner for Justice, Consumers and Gender Equality  
European Commission  
Rue de la Loi 200  
1049 Bruxelles

**Subject: EU-US Privacy Shield. Draft Commission Implementing Decision on the act on the adequacy of protection provided by the EU-US Privacy Shield**

Dear Commissioner,

I would like to draw your attention to the above-mentioned draft Commission implementing Decision on the adequacy of protection provided by the EU-US Privacy Shield.

According to information published by several press media, the Commission has issued a revised version of the draft Commission adequacy decision following "a number of additional clarifications and improvements" made after discussions with the US authorities. According to these media, this revised draft text has been notified to the Member States on 23/24 June in view of the meeting of the Committee of the Article 31, scheduled 29 June and 4 July 2016. Finally, the media have been briefed by Commission officials on the "breakthrough" realised in the discussion between the EU and US negotiators.

It appears from the procedure followed that the European Parliament has not been notified at the same time as the information was made available to the Committee 31 members. Indeed, as checked on 27 June 2016 the latest version of the draft implementing act included in the Comitology register bears the date of 14 March 2016.

Regulation (EU) N°182/2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers, lays down in Article 10 the information on committee proceedings.

Article 10(4) provides that "At the same time as they are sent to the committee members, the Commission shall make available to the European Parliament and the Council the documents referred to in points (b) (agendas), (d) (the draft implementing act) and (f) (the final draft implementing following the opinion of the committee) of paragraph 1 whilst also informing them of the availability of such documents."

I find very regrettable that the European Parliament has not been given access to information on the basis of existing legal provisions and interinstitutional agreements. This situation is in breach of the rules provided for in Regulation (EU) N° 182/2011, of the Agreement between the Parliament and the Commission on procedure for implementing Council decision 1999/468/EC laying down the procedures for the exercise of implementing powers conferred on the Commission, as amended by Decision 2006/512/EC as amended on 22.7.2006, namely its Article 1 and of the principles of sincere cooperation and transparency.

I would like to recall that, pursuant to the Interinstitutional agreement between the European Parliament, the Council of the European Union and the European Commission of 13 April 2016 on Better Law-Making, the three institutions - including the Commission - committed to sincere and transparent cooperation throughout the entire legislative cycle and recalled "in this context (...) the equality of both co-legislators as enshrined in the Treaties".

Moreover this way of doing prevents the Parliament from properly conducting its right of scrutiny, as provided for in Article 11 of Regulation (EU) N° 182/2011; therefore I urge you to do the necessary to transmit without delay to the European Parliament all relevant information regarding the draft Commission implementing act, particularly the latest reviewed version as well as any other information transmitted to the members of the Committee 31. I would also request your presence to inform the LIBE Committee about this draft implementing act.

Yours sincerely,



Claude MORAES

CC: Mr Martin Schulz, President of the European Parliament  
Mr Jerzy Buzek, Chairman of the Conference of Committee Chairs  
Mr Frans Timmermans, 1st Vice-President of European Commission



**VĚRA JOUROVÁ**  
*Member of the European Commission*

Brussels,  
Ares(2016)

Dear Mr Moraes,

Thank you for your letter of 28 June drawing my attention to press reports on the Commission's revised draft adequacy decision on the EU-U.S. Privacy Shield. .

I would like to clarify that the consolidated draft adequacy decision, including a complete version of its annexes (i.e. the documents agreed with the US that constitute the Privacy Shield), was transmitted to Member States (Article 31 committee) on Monday, 27 June. On the same day, Commission services then uploaded the full package (decision plus annexes) in the Comitology register.

I hope that this satisfactorily addresses your concerns. More generally, let me assure you that the Commission is mindful of the applicable rules, including the commitment to sincere and transparent cooperation between our two institutions, and that it takes them very seriously.

Let me also take the opportunity to inform you about what we have achieved following the publication of the original draft decision at the end of February. Further negotiations with the U.S. government and a revision of the draft decision have resulted in an overall package that provides a number of improvements and clarifications.

These reflect the various points raised by the European Parliament in its resolution of 24 May 2016, including: (i) further representations and assurances from the U.S. Office of the Director of National Intelligence (ODNI) on the limitations applicable in case of bulk collection, which show the difference to indiscriminate, mass surveillance; (ii) additional commitments strengthening the functional independence of the Ombudsperson and a further clarification of its cooperation with other independent oversight bodies with investigatory powers; (iii) a better explanation of the various alternative redress avenues available to individuals when they believe that a Privacy Shield company has not complied with its obligations under the Shield; (iv) a clear commitment on the side of the Commission to assess the level of protection provided by the Privacy Shield once the General Data Protection Regulation becomes applicable; (v) other improvements that address all of the central points raised by the Article 29 Working Party, including a new principle of limited data retention.

Mr Claude Moraes  
European Parliament  
Committee on Civil Liberties, Justice and Home Affairs  
The Chairman  
IP-LIBE@europarl.europa.eu

Again, I hope that these further changes satisfactorily address your concerns.

The Commission intends to adopt the revised adequacy decision following the vote of the Article 31 committee on 8 July. Putting in place the EU-U.S. Privacy Shield is essential to ensure a high level of protection for EU individuals, while providing legal certainty for transatlantic commercial data flows.

The Commission is available to brief your committee in detail on the revised adequacy decision.

Yours sincerely,



Věra Jourová

COMMISSION EUROPÉENNE



Bruxelles, le  
C(2016) final

Monsieur le Président,

*La Commission tient à remercier l'Assemblée nationale pour son avis concernant la communication de la Commission «Flux de données transatlantiques: rétablir la confiance grâce à des garanties solides» {COM(2016)117} et l'accord de protection des données personnelles «bouclier de protection» entre les Etats-Unis d'Amérique et l'Union européenne.*

*La Commission a adopté, le 12 juillet dernier, la décision d'exécution relative à l'adéquation de la protection assurée par le «bouclier de protection des données» UE-USA (C(2016) 4176 final), à la suite de l'avis positif émis, le 8 juillet 2016 dans le cadre du comité de l'article 31, par une très large majorité d'États membres. La décision a été notifiée aux États membres ce même 12 juillet et est, de ce fait, entrée en vigueur à cette date. La décision 2016/1250 a été publiée dans le Journal officiel de l'Union européenne le 1 août 2016.*

*Cette décision est le fruit d'un processus décisionnel dans lequel sont intervenus les États membres, les autorités nationales de protection des données (dans le cadre du «groupe de travail article 29»), le contrôleur européen de la protection des données et le Parlement européen. Prenant en compte les observations et recommandations formulées par ces différents acteurs – lesquels ont soulevé des questions similaires à celles contenues dans votre avis – sur le projet initial publié à la fin du mois de février, la Commission a repris les négociations avec les autorités américaines afin d'obtenir des précisions supplémentaires et des améliorations du «bouclier de protection des données».*

*L'objectif de la Commission a toujours été de garantir un niveau de protection élevé des données à caractère personnel des Européens. J'ai la conviction que la décision que nous venons d'adopter répond largement aux points que vous avez soulevés dans votre avis. Je me réfère notamment à la question de l'accès pour raisons de sécurité nationale des autorités américaines aux données à caractère personnel, au sujet de laquelle la Commission a obtenu des assurances supplémentaires des États-Unis sur les limitations et garanties applicables, et notamment sur le fait que les services de renseignement américains ne se livrent pas à une surveillance massive et indiscriminée des données à caractère personnel des citoyens européens et demeurent donc dans les limites de ce qui est peut être considéré nécessaire et proportionné. En ce qui concerne la création d'un nouveau mécanisme de recours, à travers l'institution d'un médiateur/ombudsperson, nous avons, sur cet aspect également, obtenu des engagements supplémentaires renforçant et précisant son indépendance fonctionnelle. Ainsi, outre à être totalement indépendant de la communauté du renseignement, le médiateur*

*M. Claude BARTOLONE  
Président de l'Assemblée nationale  
Palais Bourbon  
126, rue de l'université  
F – 75007 PARIS*

*exercera ses fonctions libre de toute influence indue pouvant affecter l'objectivité de son analyse. La manière dont ce médiateur coopérera avec d'autres organes de supervision et d'enquête indépendants a également été précisée, en clarifiant notamment que le médiateur devra obtenir toutes les informations nécessaires pour le traitement des plaintes des utilisateurs européens.*

*S'agissant ensuite des transferts ultérieurs vers des pays tiers, le projet initial prévoyait déjà que le bénéficiaire de tels transferts doit garantir le même niveau de protection que dans le cadre du «bouclier de protection des données», assurant ainsi que la «protection suit les données» indépendamment du nombre d'opérateurs intervenant dans la chaîne de traitement et de leur lieu d'établissement. À la suite des observations formulées par les parties intéressées, nous avons réussi à introduire une condition supplémentaire selon laquelle les entreprises membres du «bouclier» doivent inclure dans leurs contrats avec des tiers bénéficiaires de transferts ultérieurs une obligation requérant que ces tiers les informent s'ils ne sont plus à même de garantir ledit niveau de protection et que, dans ce cas, les transferts soient suspendus ou d'autres mesures équivalentes soient prises.*

*En ce qui concerne les recours individuels, la décision de la Commission fournit de plus amples informations sur le fonctionnement des différents mécanismes de recours dont disposent les utilisateurs européens. En particulier, la décision clarifie qu'un individu n'a pas à épuiser tous ces mécanismes, selon un ordre particulier, afin d'obtenir réparation. La Commission publiera sous peu un «guide du citoyen» pour expliquer aux citoyens de l'UE, de manière simple et accessible, les droits dont ils bénéficient et les possibilités de recours pouvant être exercés dans le cadre du «bouclier».*

*Enfin, la décision d'adéquation prévoit que la Commission contrôlera de manière régulière l'application du «bouclier» et, en particulier, le respect des engagements souscrits aussi bien par les entreprises que par les autorités américaines. Ce contrôle continu est combiné avec une clause de suspension renforcée. En outre, le mécanisme de réexamen annuel conjoint entraînera une évaluation approfondie du fonctionnement de l'ensemble des éléments du «bouclier de protection des données», y compris de ceux relatifs à l'accès des autorités américaines aux données transférées depuis l'UE. Les autorités européennes chargées de la protection des données seront pleinement associées à ce réexamen, et la Commission tiendra les États membres et le Parlement européen informés tout au long du processus. La version finale de la décision d'adéquation prévoit aussi, comme vous le suggérez, que la Commission évaluera l'impact de l'entrée en application en 2018 du nouveau cadre législatif européen en matière de protection des données sur le niveau de protection assuré par le «bouclier», et en particulier si des adaptations de cet instrument seront nécessaires.*

*En espérant que ces éclaircissements répondront aux questions soulevées par l'Assemblée nationale, nous nous réjouissons, par avance, de la poursuite de notre dialogue politique.*

*Veuillez en outre agréer, Monsieur le Président, l'expression de notre très haute considération.*

Frans Timmermans  
Premier vice-président

Věra Jourová  
Membre de la Commission

The Commission will continuously monitor the EU-U.S. Privacy Shield framework and conduct an annual joint review, which will cover all aspects of the functioning of the EU-U.S. Privacy Shield, including the U.S. commitments with respect to access to data on law enforcement and national security grounds. On the basis of this annual joint review, the Commission will report to the European Parliament and the Council.

I look forward to our continued cooperation in ensuring a high level of data protection for transatlantic transfers of personal data.

Yours sincerely,

A black rectangular box redacting the signature of Věra Jourová.

Věra Jourová

VĚRA JOUROVÁ  
Member of the European Commission

Ref. Ares(2016)5135809 - 09/09/2016

Brussels,  
Ares(2016)

Dear Mr Moraes, *Dear Claude,*

following the adoption of the Commission decision on the EU-U.S. Privacy Shield<sup>1</sup> on 12 July 2016, I would hereby like to inform you that the EU-U.S. Privacy Shield framework became operational on 1 August 2016.

Since that date, U.S. companies have been able to register with the U.S. Department of Commerce, which has been verifying that the companies' privacy policies comply with the high data protection standards required by the Privacy Shield. As at 31 August 2016, 103 companies have been certified. According to information provided by the U.S. Department of Commerce, it is currently reviewing the privacy policies of a further 190 companies that have signed up to the Privacy Shield while an additional 250 companies are in the process of submitting their application.

The EU-U.S. Privacy Shield framework ensures a high level of protection for EU individuals whose data is transferred to the U.S. for commercial purposes, while ensuring legal clarity and simplification for European businesses, especially SMEs. European companies can easily check on the Privacy Shield<sup>2</sup> list whether their American partner companies are certified under the Privacy Shield and hence that personal data can be transferred to them in compliance with EU data protection rules.

Also on 1 August, the Commission published a citizens' guide<sup>3</sup> explaining how individuals' data protection rights are guaranteed under the Privacy Shield and what remedies are available for individuals, if they consider their data has been misused and their data protection rights have not been respected. The citizens' guide is now available in all EU languages.

Mr Claude Moraes  
European Parliament  
Committee on Civil Liberties, Justice and Home Affairs  
The Chairman  
IP-LIBE@europarl.europa.eu

<sup>1</sup> 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

<sup>2</sup> <https://www.privacyshield.gov/list>

<sup>3</sup> [http://ec.europa.eu/justice/data-protection/document/citizens-guide\\_en.pdf](http://ec.europa.eu/justice/data-protection/document/citizens-guide_en.pdf)

The Commission will continuously monitor the EU-U.S. Privacy Shield framework and conduct an annual joint review, which will cover all aspects of the functioning of the EU-U.S. Privacy Shield, including the U.S. commitments with respect to access to data on law enforcement and national security grounds. On the basis of this annual joint review, the Commission will report to the European Parliament and the Council.

I look forward to our continued cooperation in ensuring a high level of data protection for transatlantic transfers of personal data.

Yours sincerely,

A black rectangular box redacting the signature of Věra Jourová.

Věra Jourová

Brussels,  
Ares(2016)

Dear Minister,

following the adoption of the Commission decision on the EU-U.S. Privacy Shield<sup>1</sup> on 12 July 2016, I would hereby like to inform you that the EU-U.S. Privacy Shield framework became operational on 1 August 2016.

Since that date, U.S. companies have been able to register with the U.S. Department of Commerce, which has been verifying that the companies' privacy policies comply with the high data protection standards required by the Privacy Shield. As at 31 August 2016, 103 companies have been certified. According to information provided by the U.S. Department of Commerce, it is currently reviewing the privacy policies of a further 190 companies that have signed up to the Privacy Shield while an additional 250 companies are in the process of submitting their application.

The EU-U.S. Privacy Shield framework ensures a high level of protection for EU individuals whose data is transferred to the U.S. for commercial purposes, while ensuring legal clarity and simplification for European businesses, especially SMEs. European companies can easily check on the Privacy Shield<sup>2</sup> list whether their American partner companies are certified under the Privacy Shield and hence that personal data can be transferred to them in compliance with EU data protection rules.

Also on 1 August, the Commission published a citizens' guide<sup>3</sup> explaining how individuals' data protection rights are guaranteed under the Privacy Shield and what remedies are available for individuals, if they consider their data has been misused and their data protection rights have not been respected. The citizens' guide is now available in all EU languages.

Ms Lucia Žitňanská  
Minister of Justice of the Slovak Republic

---

<sup>1</sup> 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

<sup>2</sup> <https://www.privacyshield.gov/list>

<sup>3</sup> [http://ec.europa.eu/justice/data-protection/document/citizens-guide\\_en.pdf](http://ec.europa.eu/justice/data-protection/document/citizens-guide_en.pdf)



The Commission will continuously monitor the EU-U.S. Privacy Shield framework and conduct an annual joint review, which will cover all aspects of the functioning of the EU-U.S. Privacy Shield, including the U.S. commitments with respect to access to data on law enforcement and national security grounds. On the basis of this annual joint review, the Commission will report to the European Parliament and the Council.

I look forward to our continued cooperation in ensuring a high level of data protection for transatlantic transfers of personal data.

Yours sincerely,

Věra Jourová



**EUROPEAN COMMISSION**  
DIRECTORATE-GENERAL JUSTICE AND CONSUMERS  
Directorate C : Fundamental rights and Union citizenship  
Unit C.3 : Data protection

**Committee on the Protection of Individuals  
with regards to the processing of Personal Data**

**(Article 31 Committee)**

**Minutes of the 62<sup>nd</sup> meeting**

**11 November 2015**

The minutes of the previous meeting were adopted and the agenda was approved.

The Commission presented the progress in its talks with the United States on a new data protection arrangement for transatlantic data transfers, following the invalidation by the Court of Justice on 6 October 2015 of the Commission Decision from the year 2000 concerning the US Safe Harbour framework (2000/520/EC).

Several Member States asked for additional explanations regarding a few aspects of the ongoing talks. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

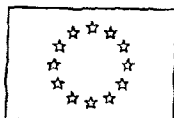
[REDACTED]

[REDACTED] informed the Committee of a recent visit of a member of their government to the U.S. and enquired about the impact of invalidating the Safe Harbour on the market position of U.S. companies in Europe. [REDACTED] underlined the need to quickly agree the new framework with the U.S. and was interested in the possible consequences of the Court ruling on other adequacy decisions. The Commission informed that Article 3 of those decisions would indeed need to be amended.

■ stressed the importance of improving the structure of the framework, given that the text of the Safe Harbour Decision of 2000, with several annexes and letters attached, was not clear. ■ also regretted that the Commission had not intervened on the Microsoft case in the U.S. courts. The Commission explained that it rarely intervenes in courts cases and even when it sometimes does, this would only be in the last instance, even in the Courts of the Member States.

■ enquired about the possible impacts of the ruling on international agreements and on the EU data protection reform. ■ pointed to some difficulties that DPAs might face when assessing data protection rules in third countries. ■ was interested in any interim measures replacing the invalidated Safe Harbour and ■ was interested in a legal analysis following the Court ruling. COM pointed to its Communication of 6 November 2015 (COM(2015) 566) which explains in depth the alternative legal grounds for data transfers to third countries in the absence of an adequacy decision.

The Commission requested members of the Article 31 Committee to provide it with information on the "best practices" in Member States regarding judicial oversight in the context of their national security activities. It invited the Member States to consider a better use of their bilateral channels with the U.S. to support the Commission's ongoing talks with the U.S.



**EUROPEAN COMMISSION**  
DIRECTORATE-GENERAL JUSTICE AND CONSUMERS

Directorate C : Fundamental rights and Union citizenship  
Unit C.3 : Data protection

**Committee on the Protection of Individuals  
with regard to the processing of Personal Data**

**(Article 31 Committee)**

**Minutes of the 63<sup>rd</sup> meeting**

**15 January 2016**

The minutes of the previous meeting were adopted and the agenda was approved.

The Commission provided the state of play in its talks with the United States on a new data protection arrangement for transatlantic data transfers since the last update to the Committee on 11 November 2015.

During the subsequent discussion, a number of MS representatives [REDACTED] highlighted the importance of finding a solution as soon as possible; asked for clarifications on the potential role of data protection authorities in the overall framework in terms of oversight of U.S. companies; and asked about the timeframe for concluding talks with the U.S.

The Commission explained that the open issues included the question of oversight of companies and enforcement in the commercial field, including by EU data protection authorities; national security exemptions and oversight in that sector; and transparency reports by companies on the number of national security and law enforcement access requests.

The Commission referred to a new and recent element in talks, namely a proposal by the U.S. to create an ombudsperson mechanism to hear complaints on national security. However, the details were still to be fleshed out. It also indicated that the U.S. seemed to be showing a greater willingness to move on a number of points and that the objective was to conclude the talks by end-January. More work was still needed to fine-tune and wrap up a number of issues before arriving to a satisfactory result in that timeframe.

The Commission concluded by assuring Member States that it will keep them informed of developments in the coming weeks.



**EUROPEAN COMMISSION**  
DIRECTORATE-GENERAL JUSTICE AND CONSUMERS

Directorate C : Fundamental rights and Union citizenship  
Unit C.3 : Data protection

**Committee on the Protection of Individuals  
with regard to the processing of Personal Data**

**(Article 31 Committee)**

**Minutes of the 64th meeting**

**7 April 2016**

**1. Adoption of the draft Agenda**

The agenda of the meeting of 7 April 2016 was approved.

**2. Adoption of the draft minutes**

The minutes of the previous meeting of 15 January 2016 were adopted without comment.

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

The Commission presented the EU-U.S. Privacy Shield framework published on 29 February 2016. This comprises (i) a draft Commission decision finding that the Privacy Shield framework provides an adequate level of data protection, and (ii) its related annexes that make up the framework, namely the Privacy Principles and Supplemental Principles which U.S. companies must comply with to receive personal data from the EU (Annex II) and the commitments by various U.S. public authorities to monitor and enforce the Privacy Shield (Annex I and III to VII).

The Commission explained that there are four main areas of improvement compared to the former Safe Harbour which the Privacy Shield replaces. These are:

(1) Stronger obligations on U.S. companies and stronger oversight and enforcement by U.S. authorities: companies that certify under the new framework will have to comply with a stronger set of Privacy Principles to ensure that personal data transferred to the U.S. is sufficiently protected and individual rights are guaranteed. The Privacy Principles and Supplemental Principles (Annex II) are now clearer, more detailed and more transparent. Tightened conditions and strict liability provisions for so called "onward transfers" have been introduced thereby ensuring the continuity of data protection

safeguards when EU personal data are transferred to third parties outside the framework, for instance for sub-processing activities. Liability stays in principle with the Privacy Shield company. As a result, the individual will only face one interlocutor when there is an issue of potential non-compliance.

In terms of oversight and enforcement of U.S. companies' compliance with the framework, the U.S. Department of Commerce, which will administer the Privacy Shield, has committed to a regular and rigorous monitoring of companies' compliance throughout the entire cycle of their participation in the framework (Annex I). It will carry out periodic ex officio compliance reviews and assessments of the program or whenever EU individuals lodge a complaint, actively pursue companies that falsely claim adherence to the scheme, strike non-compliant companies off the Privacy Shield list, indicating the reasons why they were delisted. Companies will also be subject to enforcement action, including sanctions for unfair and deceptive trade practices, by the Federal Trade Commission (Annex IV).

(2) Limitations and safeguards on surveillance and access to data by U.S. authorities (Annexes VI and VII): clear written assurances from the U.S. Government that access by public authorities to personal data transferred from Europe will be limited to what is necessary and proportionate, these principles being reflected in the U.S. concepts and policies of "tailoring" and "targeting" introduced in their recent intelligence reforms notably the 2014 Presidential Policy Directive 28 (PPD-28) and the 2015 USA Freedom Act. The documents in the Privacy Shield build on these recent developments in U.S. law and further clarify the applicable safeguards and their scope. This is a major and unprecedented difference between the Safe Harbour and the Privacy Shield. These representations from the U.S. concern in particular that they do not engage in indiscriminate mass surveillance; that they will always prioritise targeted over bulk collection of data, and only use bulk collection where targeted access is not possible for technical or operational reasons (and even then access is allowed only for a limited set of specific purposes and will be targeted through the use of specific "selectors"); extension to non-U.S. persons of a number of safeguards for individuals (e.g. minimisation, retention periods); the application of a comprehensive system of checks and balances concerning the purposes, collection and use of the data and the persons who are authorised to have access.

(3) Effective protection of privacy rights with several individual redress possibilities in both the commercial and the national security areas: the aim is to ensure that any individual complaint will be followed-up and resolved.

*In the commercial area:*

- companies have clear deadlines to reply to individuals' complaints (within 45 days);
- individuals can take a complaint to alternative dispute resolution bodies (ADRs) at no cost to them. The 'free of charge' element is a big improvement compared to the previous system.
- individuals can also take their complaints to the EU national data protection authorities (DPAs) who will refer their cases to the U.S. Department of Commerce (via a dedicated contact point) and the Federal Trade Commission for further investigation and resolution. The new framework thus opens up and strengthens the cooperation channels between the enforcers on both sides of the

Atlantic. There is a clear process and a set deadline (90 days) for the Department of Commerce to respond to DPAs when they channel a complaint from an EU data subject.

- Privacy Shield Panel (Annex to Annex II): if a case is not resolved by any of the above avenues, individuals will be able to have recourse, as a last resort, to a new dispute settlement body which would be able to decide on unresolved complaints through a binding and enforceable decision. The Panel will be a fair mechanism based on rules that fully take into account the specific situation of an individual bringing a complaint against a company, e.g., arbitration costs will be covered by a fund financed by the Privacy Shield companies rather than borne by individuals, individuals can receive assistance from their DPA to prepare their case, interpretation and translation will be provided etc.

*In the national security area:*

- the U.S. government will create a new redress mechanism allowing individuals to bring complaints in the area of national security (Annex III). The Ombudsperson mechanism at the U.S. Department of State will be independent from the national intelligence services, will be under an obligation to follow-up on complaints or enquiries from EU individuals, respond in a timely manner, and in particular confirm to the individual that the relevant laws have been complied with or that any non-compliance has been remedied. It was important to view the functioning of the mechanism in its entirety i.e. the Ombudsperson working together with other U.S. oversight bodies, in particular the Inspectors-General, who are both fully independent and have investigatory powers (e.g. to request documents, hear witnesses, carry out audits, etc.). Together, the Ombudsperson and the Inspectors-General guarantee an oversight that is both independent and has the necessary powers. Furthermore, the confirmation that the Ombudsperson has to provide to an individual necessarily requires that it will have to receive relevant and sufficient information from the Inspectors-General to allow for an own assessment, both as regards the investigation carried out and the compliance of the respective national intelligence activities with U.S. law. Finally, the mechanism extends to all personal data and all types of transfer i.e. whether transferred under the Privacy Shield or alternative transfer tools. Again, this is a novel and unprecedented feature of the Privacy Shield, even more so given that it is in the national security area.

(4) Annual joint review mechanism: the Commission will regularly monitor the functioning of all aspects of the Privacy Shield, checking whether the U.S. commitments are complied with and whether the various oversight and redress mechanisms (from the Privacy Shield Panel to the Ombudsperson) are operating effectively. The Commission and the Department of Commerce will conduct this exercise through an annual joint review, which will involve EU DPAs as well as national security experts from the U.S. and the Ombudsperson as necessary. The information gathered during this review will then allow the Commission to assess the situation and report to the European Parliament and the Council. Furthermore, the Commission draft decision now contains clear parameters and detailed conditions under which it can suspend or repeal the decision in case either U.S. companies or authorities fail to fulfil their obligations under the Privacy Shield.

The Commission then noted that the Article 29 Working Party (WP29) of national DPAs was in the process of finalising its opinion on the Privacy Shield which will be adopted at the plenary session on 12-13 April 2016. Their opinion will be forwarded to the Article

31 Committee. The European Data Protection Supervisor is also expected to draw up an opinion towards the end of April [note: in the meantime the date has been postponed to the period 11-17 May].

The Commission announced that additional meetings of the Article 31 Committee were scheduled for 29 April and 19 May 2016. Finally, the Commission expressed the hope that Member States will take a favourable view of the adequacy of the Privacy Shield framework.

The Member States that subsequently took the floor [REDACTED] [REDACTED] were supportive of the Commission's efforts to conclude a comprehensive data transfer framework with the U.S., welcomed the important improvements when compared to the Safe Harbour and hoped that the framework could be adopted soon. At the same time, a number of critical questions were raised by some delegations, notably:

- the impact of a possible negative opinion from the WP29: COM replied that it will carefully and seriously study the WP29 opinion as it will study the opinion of this Committee, pointing out that it may be possible to clarify/elaborate things in the adequacy decision itself without necessarily reopening negotiations as such.
- complexity of the Privacy Shield due to the number of annexes (seven in all) and interlinked rules dispersed across the texts, in particular as regards the available redress mechanisms: COM said it would be willing to provide more clarity at the next meeting by pointing Member States to the relevant parts in the texts, including with regard to the redress mechanisms.
- procedural rules of the DPA Panel and whether U.S. companies could choose between ADRs in the U.S. or DPAs in the EU: COM pointed to the "basic rules" in point 5(c) of the Supplemental Principles vis-à-vis the DPA Panel. It recalled that this panel also existed in the former Safe Harbour and established a set of procedural rules that could form a basis for the rules to be established under the Privacy Shield. Under the Notice Principle, companies are obliged to indicate the free-of-charge independent dispute resolution body designated to address complaints which could be the DPA Panel, an ADR based in the EU or one based in the U.S. However, for human resources data, companies are obliged to commit to cooperate with EU DPAs to handle complaints.
- possibility for a "dispute resolution body" to award compensation: COM explained that compensation is not envisaged; DPAs themselves do not dispense compensation. Under U.S. civil law, however, it is possible to bring a civil action for damages.
- whether a change of U.S. administration would compromise the establishment of the Ombudsperson and/or result in the appointment of a new one: COM explained that the U.S. has undertaken a serious commitment to set this up and, as with all other commitments under the Privacy Shield, expects that the Privacy Shield framework will continue to operate as expected irrespective of which administration is in power or who the individual fulfilling the Ombudsperson role actually is. This has been the case with the Safe Harbour (which lasted for 15 years).



- whether the COM intends to set up the "EU complaint handling body" referred to in the Ombudsperson mechanism: COM stated that we would first want to gain some experience with the role of national bodies to channel individuals' complaints to the Ombudsperson to see whether there is a need to centralise the system.
- for onwards transfers, whether individuals can opt-out of having their data transferred when there is a change of purpose: COM replied that the contract provided for in the onward transfer principle between controllers and controllers and controllers and processors must fully ensure the same level of protection as in the Privacy Shield, including the opt-out clause in the Choice Principle, which includes the possibility to object to a different purpose.
- question as to why the Privacy Principles will be interpreted according to US law: COM replied this is because, like the Safe Harbour before it, the Privacy Shield framework is a U.S. framework, administered and enforced by U.S. authorities in the U.S.
- need for "re-admission" of U.S. Safe Harbour companies to the Privacy Shield: COM pointed out that as the Safe Harbour had been invalidated, there is no automatic 'roll-over' to the Privacy Shield which is a new framework.
- interaction between the responsibilities of U.S. companies under the Privacy Shield and the future General Data Protection Regulation (GDPR) when offering goods and services in the EU: COM explained that there is no overlap as the Privacy Shield only applies where the GDPR does not, namely once data have been transferred from an EU controller to the U.S.
- review of the Commission decisions on model clauses: COM indicated that it has no fixed plans as yet to review these decisions.

The Committee will continue its discussion of the Privacy Shield framework at the next meetings.

#### **4. Any other business:**

No other issues were raised.

\* \* \*



**EUROPEAN COMMISSION**  
DIRECTORATE-GENERAL JUSTICE AND CONSUMERS

Directorate C : Fundamental rights and Union citizenship  
Unit C.3 : Data protection

**Committee on the Protection of Individuals  
with regard to the processing of Personal Data**

**(Article 31 Committee)**

**Minutes of the 65th meeting**

**29 April 2016**

**1. Adoption of the draft Agenda**

The agenda of the meeting of 29 April 2016 was approved.

**2. Adoption of the draft minutes**

The minutes of the meeting of 7 April 2016 were adopted as amended following a comment by SI.

**3. The EU-U.S. Privacy Shield**

The meeting was a follow-up to the Commission presentation on the Privacy Shield of 7 April 2016 and aimed at discussing in more detail the consequences to be drawn from the Opinion of the Article 29 Working Party (WP29) as well as additional comments from the Member States on the Commission draft adequacy decision and the underlying Privacy Shield documents drawn up by the U.S. government.

The Members took note of the WP29 opinion adopted on 13 April 2016. The Commission presented the way forward to address some of the issues raised by the WP29, both on the commercial side and as regards access by U.S. public authorities for national security purposes.

The Commission informed the Committee that in its view some issues could be resolved unilaterally through clarifications in the adequacy decision and that it intends to prepare a 'citizen guide' to explain e.g. the redress mechanisms. Other issues require improvements in the underlying U.S. texts (i.e. the Annexes) and therefore an agreement with the U.S. side. The Commission also informed about its preliminary exchanges of views with the U.S. on the work yet to be done on the texts.

Some Members States informed about their recent bilateral contacts with the U.S. government.

The following Member States supported the Commission's approach, provided further comments or requested clarifications on the Privacy Shield: [REDACTED]

[REDACTED]. A number of them underlined the importance of putting in place, without delays, a strong and sustainable legal framework. The discussion on the national security aspects focused thereafter on two themes: (1) the Ombudsperson - better explaining its composite structure and further clarifications and improvements in the current text, notably as regards functional independence and cooperation with other independent oversight bodies as well as the possibility of channelling complaints through EU national data protection authorities; (2) improvements to the ODNI letter that would further clarify the limitations applying to the "bulk collection" of data in view of addressing the remaining concerns relating to "massive and indiscriminate surveillance".

A number of Member States expressed support to include new provisions on data retention and automated processing. Member States also discussed issues related to onward transfers of personal data, the Privacy Shield Panel, the annual joint review. The feasibility of revisiting the Privacy Shield when the General Data Protection Regulation will become effective and applied was raised. They also requested more clarity on the redress mechanisms available to individuals and the Commission indicated that it would prepare an overview that lays out the various redress avenues and guides through the annexes.

The Commission explained that for the moment it maintains the target date for the adoption of the decision in June but cautioned that the date depends on the U.S. government understanding the need to address promptly the remaining issues.

#### **4. Any other business:**

The Commission proposed to hold the next meeting on 19 May 2016.

\* \* \*



**EUROPEAN COMMISSION**  
DIRECTORATE-GENERAL JUSTICE AND CONSUMERS

Directorate C : Fundamental rights and Union citizenship  
Unit C.3 : Data protection

**Committee on the Protection of Individuals  
with regard to the processing of Personal Data**

**(Article 31 Committee)**

**Minutes of the 66th meeting**

**19 May 2016**

**1. Adoption of the draft Agenda**

The agenda of the meeting of 19 May 2016 was approved.

**2. Adoption of the draft minutes**

The minutes of the meeting of 29 April 2016 were adopted pending a request for an amendment from AT.

**3. The EU-U.S. Privacy Shield**

The Commission briefed the Members of the Committee on the state of play of its talks with the U.S. since the last meeting on 29 April 2016, notably on possible changes to the U.S. documents forming the Privacy Shield and annexed to the draft Commission decision, which can only be achieved in agreement with the U.S. government. The Commission informed Members that so far the U.S. has provided additional clarifications on the issue of bulk collection of data, which was a positive development. The U.S. had further indicated that it generally agrees on the need to introduce an explicit principle on limiting data retention and an obligation to inform the COM of changes in their legislation possibly affecting the Privacy Shield but had not yet put forward any textual proposals in response to those provided by the Commission. [REDACTED]

Talks with the U.S. are ongoing. The Commission urged Member States to continue to stress the importance of these issues in their bilateral contacts with the U.S. in order for them to be able to fully endorse the Privacy Shield framework and to give a positive opinion.

The Commission reported that the EDPS would be issuing its opinion on the Privacy Shield at the end of May while the European Parliament would be voting on a resolution on 25 May 2016.

The majority of Members that intervened supported the Commission's approach to seek a number of improvements/clarifications to the U.S. texts and underlined the importance of obtaining a solid framework [REDACTED] Some of those that had already had contacts with the U.S. said they would continue to convey the urgency to the U.S. on the need to improve the texts on a number of key aspects if we wanted to maintain the momentum to adopt the decision by the summer.

Some of the specific points raised during the subsequent discussion included:

- [REDACTED] expressed its appreciation for the Commission's helpful briefing made on 17 May explaining the Privacy Shield to their parliamentary committee. They asked whether the adequacy decision could systematically address the points raised in the *Schrems* judgment and whether model contracts would be developed for onward transfers. On the first point, the Commission replied the Court had criticised the Safe Harbour decision for lacking a reasoned assessment on its adequacy whereas now the recitals in the draft Privacy Shield decision explained the various point in detail. On the second point, the Commission replied that as these contracts would fall under U.S. law the Commission is not competent to develop specific models. [REDACTED] supported the drafting of an explanatory guide for citizens and business.
- [REDACTED] had concerns as regards bulk collection and the Ombudsperson mechanism and was pleased to hear that there was some progress on the first point.
- [REDACTED] informed that it would be providing written amendments to the draft decision including on data retention and onward transfers, the role of DPAs in redress mechanisms as well as language concerning the possibility to review the Privacy Shield once the General Data Protection Regulation (GDPR) will apply, while explaining that they were not asking for a sunset clause. [REDACTED] also enquired about the possibility of developing a glossary of terms. The Commission was open to receiving suggestions for possible amendments without, however, opening new issues. It indicated that a glossary could possibly be provided in the citizens' guide.
- [REDACTED] asked for better explanations with possible examples regarding bulk collection in the Commission decision and whether it would be possible to make any changes in Recital 102 (on the Ombudsperson) with respect to the involvement of data protection authorities.
- [REDACTED] highlighted the usefulness of a guide providing orientation as regards the content of the annexes and enquired on the possible link of the Privacy Shield with other transatlantic files (essentially TTIP). On the latter point, the Commission said that the issues are kept separate.
- [REDACTED] stated its preference, in view of the entry into application of the GDPR in 2018, for a strong revision clause and suggested a review within three years of the application of the Regulation. The Commission explained that this is not necessary in its view given that the draft adequacy decision foresees a strong

suspension clause and the Privacy Shield annual joint review. In addition, a provision whereby the U.S. must inform of changes in their law that materially affect the Privacy Shield is under negotiation. This replied to the Court's criterion for the continuous review of an adequacy decision. A revision clause was also not desirable because companies may be discouraged from joining the Shield if it were subject to a revision too soon after adoption because of a lack of legal certainty.

[REDACTED]

[REDACTED] highlighted the importance of having a provision prohibiting decisions based on automated processing, citing competition concerns between EU and U.S. companies should they be held to different standards on profiling.

**4. Any other business:**

The Commission proposed to hold the next meeting on 6 June 2016. A further meeting has tentatively been scheduled for 20 June 2016.

\* \* \*



**EUROPEAN COMMISSION**  
DIRECTORATE-GENERAL JUSTICE AND CONSUMERS

Directorate C : Fundamental rights and Union citizenship  
Unit C.3 : Data protection

**Committee on the Protection of Individuals  
with regard to the processing of Personal Data**

**(Article 31 Committee)**

**Minutes of the 67th meeting**

**6 June 2016**

**1. Adoption of the draft Agenda**

The agenda of the meeting of 6 June 2016 was approved.

**2. Adoption of the draft minutes**

The minutes of the meeting of 19 May 2016 were adopted.

**3. The EU-U.S. Privacy Shield**

The Commission provided the Members of the Committee with a detailed update on the state of play of its talks with the U.S. since the last meeting on 19 May 2016.

The Commission reported that good progress has been made on one of the most difficult issues, namely improving the Ombudsperson mechanism in three main areas: (1) independence, where we now have new language that strengthens the functional autonomy of the Ombudsperson; (2) relationship between the Ombudsperson and the other oversight bodies, where we now have language that clarifies how the composite Ombudsperson system will function in that the investigation will be carried out by independent oversight bodies that will have to provide the Ombudsperson all the necessary information allowing her to confirm that US law has been complied with or, if not, that this has been remedied; and (3) the referral entity in the EU channelling the requests, where we now have language that ensures that data subjects will always be able to lodge their complaint with their DPA provided that the complaints are channelled to the Ombudsperson via a centralised EU body. The Commission indicated that one possibility could be for the Article 29 Working Party to have one of their members perform this function.

Together with the additional clarifications on bulk collection of data which were referred to at the previous meeting, the Commission considers that the issue of access by public

authorities satisfactorily responds to the concerns raised by Member States and the Article 29 Working Party.

[REDACTED]

The Commission presented the proposals that it had made to the US on these points explaining that these were largely based not only on our *acquis* but also on precedents in other instruments agreed with the US or on their own laws. The Commission encouraged Committee Members to continue to highlight the importance and the urgency of reaching an agreement on these points in the interest of ensuring legal certainty.

Discussion on another point relating to a commitment from the US to inform the Commission about changes in US legislation that could have an impact on the functioning of the Privacy Shield was moving in the right direction.

In the ensuing discussion, Member States raised the following issues: concerns about the recent news that the other data transfer tools (i.e. standard contractual clauses - SCCs) will most likely be challenged in court which would create again more uncertainty if they would also be invalidated [REDACTED]; the need to have the Privacy Shield in place by the summer [REDACTED]; whether the Commission intends to review existing adequacy decisions in light of the *Schrems* ruling [REDACTED]; whether the Privacy Shield adequacy decision would contain a review clause [REDACTED]. Committee Members also enquired about the likely date when they would be asked to give their opinion on the draft adequacy decision.

On the timing for the adoption of the adequacy decision, the Commission hoped the Committee could take a decision on the 29 June 2016 but much depended on the pace of discussions with the US. On the SCCs, it was not possible to speculate on the outcome of any challenge but this showed even more the importance to have as strong a Privacy Shield as possible. As to the existing adequacy decisions, the Commission recalled its intention to amend these in light of the *Schrems* ruling with respect to the powers of the DPAs. Countries covered by adequacy decision should be more proactive in providing information about material changes to their laws and the Commission asked Member States to pass on this message in their bilateral contacts.

Further meetings of the Article 31 Committee have been scheduled for 20 June and 29 June.

#### **4. Any other business:**

None.

\* \* \*





**EUROPEAN COMMISSION**  
DIRECTORATE-GENERAL JUSTICE AND CONSUMERS

Directorate C : Fundamental rights and Union citizenship  
Unit C.3 : Data protection

**Committee on the Protection of Individuals  
with regard to the processing of Personal Data**

**(Article 31 Committee)**

**Minutes of the 68th meeting**

**20 June 2016**

**1. Adoption of the draft Agenda**

The agenda of the meeting of 20 June 2016 was approved.

**2. Adoption of the draft minutes**

The Chair informed that the minutes of the meeting of 6 June 2016 are still being prepared and will be circulated at a later date.

**3. The EU-U.S. Privacy Shield**

The Commission provided the Members of the Committee with a detailed update on the state of play of its talks with the U.S. since the last meeting on 6 June 2016:

The Commission informed that it was still working on the issues of (limited) data retention and on bulk collection, and asked Member States to support its efforts in view of a successful conclusion of the negotiations.

[REDACTED] In this context [REDACTED] and [REDACTED] asked for clarifications regarding the Commission's new proposals on bulk collection while [REDACTED], [REDACTED] and [REDACTED] stated this was an important issue on which they still had concerns and needed further study. [REDACTED] questioned whether the additional U.S. text on bulk collection presented orally by the Commission fulfilled the requirements of the Court of Justice.

■ asked for clarity on which issues were still on the table.

■ expressed worries as to the risk of reopening discussions on the agreed definition of personal data. ■ and ■ asked for clarifications on the agreed text on onward transfers. ■ focused on safeguards in the area of automated processing of data.

While ■ urged adoption of the Shield before the summer, ■ indicated that from its perspective there was no hurry to conclude a deal. Several Member States, among them ■ asked whether the Commission could transmit the draft texts presented orally.

COM explained that: (i) considerable progress was reached on the issue of bulk collection, (ii) an agreement was reached on strengthening the text on the Ombudsperson, notably as regards functional independence, investigatory powers and channelling of complaints from Europe, (iii) the talks were still ongoing on a footnote related to data retention, in line with the agreed definition of personal data, (iv) an agreement had been reached on onward transfers (the third party would need to notify the Privacy Shield company if it no longer can meet its contractual obligations), and (v) ■

Several Member States enquired on the timetable of the adoption. COM explained that it was ready to close negotiations as soon as an overall compromise on all points under discussion would be reached with the U.S.

#### **4. Any other business:**

The Commission proposed to hold the next meeting on 29 June 2016.

\* \* \*



**EUROPEAN COMMISSION**  
DIRECTORATE-GENERAL JUSTICE AND CONSUMERS

Directorate C : Fundamental rights and Union citizenship  
Unit C.3 : Data protection

**Committee on the Protection of Individuals  
with regard to the processing of Personal Data**

**(Article 31 Committee)**

**Minutes of the 69th meeting**

**29 June 2016**

**1. Adoption of the draft Agenda**

The agenda of the meeting of 29 June 2016 was approved.

**2. Adoption of the draft minutes**

The Chair informed that the minutes of the meetings of 6 and 20 June 2016 were still being finalised.

**3. The EU-U.S. Privacy Shield**

COM informed members that it had finalised the negotiations with the U.S. on the Privacy Shield with satisfactory results and pointed to a number of additional commitments received from the U.S. since the previous meeting of the Article 31 Committee on 20 June 2016. They include tightened conditions for onward transfers of personal data from Privacy Shield organisations to third parties. Privacy Shield organisations will have to include in their contracts with third parties an obligation to notify the former if the latter can no longer guarantee the same level of data protection as required under the Privacy Shield. As regards automated decision-making, the U.S. had provided the COM with information about existing safeguards for individuals and consumers in their laws (namely, rules in certain sectors that ensure information about the underlying logic of the processing and a right to express a view and/or to request the correction of data); the parties also agreed that automated processing would be further

discussed during the first annual review (and possibly further annual reviews) of the Privacy Shield.

COM explained that it had now clarified the various redress possibilities offered by the new framework in the draft decision: they are all to the advantage of EU data subjects; individuals will be able to choose between them (i.e., they are alternatives); only appealing to the arbitration panel would require that the data subject first exhausts other available redress possibilities; the arbitration panel will have a number of consumer friendly features (which a typical appeal court would not be able to offer) including the possibility to participate by videoconference and to receive free of charge translation to facilitate bringing a case.

COM reminded the Committee about a number of improvements introduced since 29 February 2016, which include i.a. important clarifications on bulk collection and improvements regarding the new position of the Ombudsperson who will be dealing with complaints from EU data subjects in the context of access to data for national security purposes. As regards bulk collection, the U.S. has provided further clarifications and assurance that show the difference to mass surveillance. COM explained its view that the U.S. commitments fully comply with the requirements formulated by the CJEU in the *Schrems* case.

Committee Members agreed that substantial and important improvements had been introduced in the draft framework. A number of members signalled their willingness – subject to confirmation of their capitals – to conclude positively the decision making process by recognising the Privacy Shield as adequately protecting personal data of EU data subjects.

A discussion followed with [REDACTED] commenting on a number of provisions of the Privacy Shield and COM providing further explanations and clarifications. The following issues of the framework were discussed in more detail: the status of the Ombudsperson [REDACTED]; bulk collection [REDACTED]; compatible processing and the notion of 'identifiable person' [REDACTED]; exemptions e.g. for statistical purposes; the status of the current draft decision and the possibility of holding a public consultation [REDACTED]; the notion of 'EU data subject' [REDACTED]; the creation of an EU centralised body to channel complaints to the U.S. [REDACTED]; the publication of a Privacy Shield handbook and its timing [REDACTED]; rules for data processors [REDACTED]; key-coded data [REDACTED]; notions of 'reasonableness' in the framework [REDACTED]; onward transfers [REDACTED]; the need for additional consultations with the Article 29 Working Party [REDACTED]; an amendment recently proposed by a Senator in the U.S. Congress which (if ever adopted) might limit the PCLOB's competence to oversee intelligence services only with a view to protect the privacy of US persons [REDACTED].

#### **4. Any other business:**

[REDACTED] stressed the need to have more time to scrutinise the revised documents. COM therefore proposed to limit the next meeting on 4 July to addressing any further questions. COM will then seek the Member States' opinion at the subsequent meeting on 8 July.



**EUROPEAN COMMISSION**  
DIRECTORATE-GENERAL JUSTICE AND CONSUMERS

Directorate C : Fundamental rights and Union citizenship  
Unit C.3 : Data protection

**Committee on the Protection of Individuals  
with regard to the processing of Personal Data**

**(Article 31 Committee)**

**Minutes of the 70th meeting**

**4 July 2016**

**1. Adoption of the draft Agenda**

The agenda of the meeting of 4 July 2016 was approved.


**2. Adoption of the draft minutes**

The minutes of the meetings of 6 and 20 June 2016 were approved. The Chair informed that the minutes of the meeting on 29 June 2016 would be circulated shortly.

**3. The EU-U.S. Privacy Shield**

COM informed that it had received written questions from [REDACTED] and [REDACTED] asking for clarifications of various aspects of the Privacy Shield. COM then proceeded to answering those and other questions asked during the meeting. During the discussion, [REDACTED] took the floor. The following issues were raised:

1. Terminology: "EU citizens" vs. "EU individuals": COM answered that it would ask the U.S. to replace the term "citizens" with "individuals" in relevant parts of the Privacy Shield.
2. Judicial Redress Act: COM informed that the Act concerns data transfers between law enforcement authorities and is thus not directly relevant to "commercial" transfers under the Privacy Shield.

3. Annual reviews: COM informed that each Party, the EU and the U.S., is free to decide on the composition of its delegation to attend annual reviews.
4. GDPR and a review of the Privacy Shield: COM confirmed that the possible consequences of the GDPR for the adequacy finding will be assessed after the entry into application of the GDPR, including at the annual review in that year.
5. Onward transfers to processors and sub-processors: COM pointed out that the safeguards with respect to such transfers had been significantly strengthened compared to the Safe Harbour; a high level of data protection will apply along with liability of data controllers; processors that will be not able to maintain the same level of protection as under the Privacy Shield will have to inform data controllers who in turn would then have to take appropriate measures, including the possibility to suspend transfers.
6. Supervisory and enforcement authorities: COM described enforcement powers of the FTC (including fines), monitoring and controlling powers of the Department of Commerce and enforceable decisions delivered by the Privacy Shield Panel.
7. Legal value and binding effect of U.S. commitments: COM pointed to the official nature of the U.S. letters concerning national security, signed by high ranking officials and to be published in the Federal Register (the equivalent to the EU Official Journal); the U.S. authorities will be legally bound by their commitments under U.S. law; also, COM confirmed that the suspension clause could be triggered if commitments are not respected by the U.S. government.
8. 
9. Notice and Choice Principles: COM pointed out that those are not the only Privacy Principles that apply to data processing by Privacy Shield companies, including in the case of onward transfers. While an exception applies for a transitional period, the reason for this and why it is legally acceptable is (now) explained in the draft adequacy decision.
10. Privacy Shield vs. Standard Contractual Clauses: COM pointed out that no easy comparison can be made as each of these legal instruments provide specific safeguards which need be seen in the context of other safeguards under the same instrument, e.g enforcement by the FTC under the Privacy Shield.

11. Article 29 Working Party: COM informed Members that it had given the highest consideration to the Article 29WP Opinion, and pointed out that in line with applicable rules the COM does not intend to consult the Article 29WP once more. COM also stressed that the Chair of the Article 29WP itself had made clear that no second opinion would be issued before the adoption of the adequacy decision.
12. Annexes related to the Privacy Shield Panel: COM indicated that, while it would have preferred to have only one Annex, there was a reason for including the Annex twice, namely that it both constituted a part of the Privacy Principles (to which U.S. companies will have to sign up to) and contained commitments from the U.S. government.
13. Numbering of paragraphs in the Annex on the Arbitral Panel: COM informed the Members that it would correct the numbering.
14. Recital 23 of the draft decision on the exceptions to limited data retention: COM confirmed that it would align the description in the draft decision on the exception for archiving with the Annex (which in turn is in line with the EU data protection rules).
15. Recital 60 on powers of DPAs: COM informed that it would amend the text.
16. Citizen Guide: COM informed that the Citizen Guide (handbook) would focus on the Privacy Principles (including the corresponding rights of data subjects) and the various redress possibilities which would be presented in a clear, "simplified" way to allow for easy understanding by consumers.
17. Rules for data processors in case of onward transfers: COM confirmed that this could be discussed in the Annual Joint Review if the practice would reveal any problems not sanctioned by the U.S.
18. Key-coded data: COM confirmed that the processing of such data is not covered by the Privacy Shield.

Following the discussion and clarifications from the COM, the COM summarised the adjustments it intended to make to the draft adequacy decision and informed Members that it would re-circulate the final version of the draft decision and a revised version of the Annexes in the following day(s). COM confirmed that on 8 July it would seek a consensus of Member States and, if consensus proves not to be possible, would proceed to ask for a vote.

\* \* \*



**EUROPEAN COMMISSION**  
DIRECTORATE-GENERAL JUSTICE AND CONSUMERS

Directorate C : Fundamental rights and Union citizenship  
Unit C.3 : Data protection

**Committee on the Protection of Individuals  
with regard to the processing of Personal Data**

**(Article 31 Committee)**

**Minutes of the 71th meeting**

**8 July 2016**

**1. Adoption of the draft Agenda**

The agenda of the meeting of 8 July 2016 was approved.

**2. Adoption of the draft minutes**

The minutes of the meetings of 29 June and 4 July 2016 were approved.

**3. Draft Commission implementing decision on the EU-U.S. Privacy Shield**

COM explained that a number of limited changes had been made in the texts of the draft decision and related annexes since the last meeting of 4 July 2016 which had been communicated to Member States in the revised versions sent on 5 July (decision) and 6 July 2016 (annexes). COM also indicated some additional changes of a purely editorial nature.

COM reminded that there had been altogether eight meetings of the Article 31 Committee since the publication of the draft adequacy decision on 29 February 2016 that provided the opportunity for in-depth discussions on the draft decision and annexes, including of further improvements to the Privacy Shield introduced in the last months. The Privacy Shield is a radically different and substantially strengthened arrangement compared to the Safe Harbour framework, invalidated by the CJEU in October 2015.

COM then outlined the main features of the Privacy Shield: (1) stricter data protection obligations on companies on how they should use personal data; (2) reinforced



monitoring and enforcement by the U.S. authorities; (3) improved redress mechanisms available to individuals, including for the first time in national security through the creation of an Ombudsperson mechanism, (4) clear limitations to access to data by public authorities; (5) more effective monitoring of the framework including through an annual joint review mechanism and a clear suspension clause.

COM asked Committee Members whether they had any points or questions to raise on the substance of the Privacy Shield. Members did not raise any points or questions of substance.

Following a question from [REDACTED], COM informed that the decision will be adopted in all official languages. On the same day COM would notify the decision to all Member States. Further to a question from [REDACTED], COM informed that it is in contact with the U.S. authorities to ensure that the certification process in the U.S. would begin as soon as possible after the decision is adopted.

COM then proceeded to ask the Committee whether it was possible to seek the Committee's support for the draft decision by consensus. [REDACTED] requested that the Committee proceed to a formal vote.

A formal vote was taken and the Committee approved the draft adequacy decision with 24 Member States in favour, none against, and four abstentions [REDACTED].

Prior to the vote, [REDACTED]

[REDACTED] After the vote, [REDACTED] thanked the COM for its very hard work and requested that the following statement be entered into the minutes of the meeting:

*"[REDACTED] welcomes the latest amendments to the Commission's proposal for a Decision setting up the Privacy Shield as legal framework for the transfer of personal data of EU data subjects to the United States for commercial purposes, amendments which have taken into account the observations of the Article 29 Working Party and improved the text also in line with the indications given by the [REDACTED] Data Protection Authority. It expresses a favourable vote in the Article 31 Committee on the proposal, in the light of the clarifications given by the Commission on this framework, and in particular on the subjective scope of application of the safeguards it provides: in this respect, [REDACTED] underlines the importance of the right to protection of personal data as a fundamental human right, which must be protected regardless of the nationality of the data subject."*

[REDACTED] also on behalf of [REDACTED] requested that the following statement be entered into the minutes of the meeting:

*"[REDACTED] take note of the adoption by the Commission of the decision on the adequacy of the protection provided by the EU-US "Privacy Shield".*

*This new framework will address the legal uncertainty which resulted from the invalidation by the ECJ of the previous decision on adequacy "Safe Harbor". It provides an improved set of data protection requirements, and creates new mechanisms to secure the data flows between the EU and the US, for thousands of European companies and people.*

*Nevertheless, as the protection of fundamental rights of European data subjects, especially as regards their right to private and family life and their right to protection of personal data, is a long commitment and a matter of high priority for our governments, we will pay close attention to the monitoring of the implementation of this agreement. The annual joint review offers an adequate opportunity to maintain a close dialogue with the US, with a view to identify and solve any issue which may arise from the application of this new framework, and allow for any improvement that may be deemed necessary, especially due to the entry into application in 2018 of the new European regulation.*

██████████ emphasize on this occasion their strong commitment to promote high standards for data protection, preserving legitimate public policy objectives."

█████ noted that it would have preferred to have had more time to study the text, but believed that the decision is necessary in order to face the situation of legal uncertainty. █████ thanked the COM for its excellent work, welcomed the strong majority in favour of the framework and stated its association with the statement read out by █████.

COM reminded the Committee about the confidential nature of its deliberations, explaining that the publication of the results of the vote in the comitology register will only show the final result without indicating the position of individual Member States.

\* \* \*

Annex I: List of Participants

Annex II: Agenda of the meeting on 8 July 2016

## ANNEX 1

### LIST OF PARTICIPANTS

Country	Organisation
AT	Federal Chancellery
AT	Permanent Representation of Austria to the EU
BE	Permanent Representation of Belgium to the EU
BE	Ministry of Justice
BG	Permanent Representation of Bulgaria to the EU
CY	Permanent Representation of Cyprus to the EU
CZ	Permanent Representation of the Czech Republic to the EU
DA	Ministry of Justice
DE	Permanent Representation of Germany to the EU
DE	Federal Ministry of the Interior
DE	Vertreter Deutschland /Bundesrat
DE	Federal Commission of Data Protection
EE	Estonian Ministry of Justice
EL	Permanent Representation of Greece to the EU
ES	Permanent Representation of Spain to the EU
FI	Permanent Representation of Finland to the EU
FI	Ministry of Justice
FR	Ministère de la Justice et des Libertés
FR	Représentation permanente de la France auprès de l'Union européenne
HU	Permanent Representation of Hungary to the EU
HR	Croatian Data Protection Authority
HR	Croatian Permanent Representation
IE	Department of Justice and Equality
IT	Permanent Representation of Italy to the EU
LT	Permanent Representation of Lithuania to the EU
LV	Ministry of Justice
LU	Ministère d'Etat, Service Medias et Communication

<b>Country</b>	<b>Organisation</b>
MT	Ministry for Social Dialogue Consumer Affairs and Civil liberties
MT	Permanent Representation of Malta to the EU
NL	Ministry of Security and Justice
NL	Permanent Representation of the Netherlands to the EU
PL	Permanent Representation of Poland to the EU
PL	Ministry of Digital Affairs
PT	Ministry of Justice
PT	Permanent Representation of Portugal to the EU
RO	Permanent Representation of Romania to the EU
SE	Ministry of Justice
SI	Ministry of Justice
SK	Permanent Representation of Slovakia to the EU
UK	Department for Culture, Media and Sports
European Commission	DG Justice & Consumers (Unit C3) Chair
EEAS	Americas I Division

ANNEX 2

***Committee on the Protection of Individuals  
with regard to the Processing of Personal Data<sup>1</sup>***

***– 71<sup>st</sup> meeting, 08 July 2016 –***

***09:30 - 13:00***

***Centre Borschette (Room CCAB 2A)***

***(36 rue Froissart, 1040 Brussels)***

***Draft Agenda***

**General:**

1. Adoption of the draft agenda
2. Adoption of the draft minutes

**Proposed measures pursuant to Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data on which the Committee is asked to give an opinion, in accordance with the examination procedure provided for in Article 31 of Directive 95/46/EC:**

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

**Other issues put to the Committee for information or a simple exchange of views on the chairman's initiative:**

4. Any other business.

\* \* \*

<sup>1</sup> Set up under Article 31 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal EU L 281, 23/11/1995, p. 31 – 50.

## For Comitology Register

Ref Ares(2016)3282595 - 08/07/2016

### OVERALL VOTING RESULT ON A FORMAL OPINION

Related to draft implementing acts submitted under Regulation (EU) No 182/2011 and measures under the regulatory procedure with scrutiny under Decision 1999/468/EC<sup>1</sup>

For votes under new Lisbon rules as from 1 November 2014

Date of delivery of the opinion: 08/07/2016  
RegCom number of draft implementing act/measure: D045249/12

#### Opinion of the committee:

Positive opinion ☒ X  
Negative opinion ☐  
No opinion: following a vote: ☐  
following expiry of the time-limit for the committee to deliver an opinion: ☐

#### Type of procedure – Reg 182/2011:

Advisory (Art. 4) ☐  
Advisory (urgency, Art. 8) ☐  
Examination (Art. 5) ☒ X  
Examination (urgency, Art. 8) ☐  
Appeal Committee: (Art. 6) ☐  
Exceptional cases (Art. 7) ☐

#### Type of procedure – Dec 1999/468/EC:

Regulatory with scrutiny (Art. 5a) ☐  
Regulatory with scrutiny (urgency, Art 6) ☐

#### Advisory/ Advisory (urgency) procedure - Overall voting results:

Consensus: ☐  
Formal vote: Number of Member States in favour: [...]  
Number of Member States against: [...]  
Number of abstentions: [...]

The simple majority, which applies to the vote under the advisory procedure, is achieved with the majority of the Member States (at least 15 delegations).

#### Examination/ Examination (urgency)/appeal/regulatory with scrutiny procedure - Overall voting results<sup>2</sup>:

Consensus: ☐  
Formal vote: Number of Member States in favour: [24]  
representing a population of: [95.66%]  
Number of Member States against: [0]  
representing a population of: [0]  
Number of abstentions: [4]  
Representing a population of: [4.34%]

65% population threshold met? In favour X against ☐

Only in case the 65 % population threshold is not met:

Does the blocking minority include at least four Member States? Yes ☐ No ☐

If applicable:

<sup>1</sup> The regulatory procedure with scrutiny still applies in cases in which the basic act has not yet been aligned to the Lisbon Treaty

<sup>2</sup> In accordance with Article 16(4) TEU a **qualified majority** is defined as at least 55% of the Member States (ie. 16) comprising at least 65% of the EU population. A blocking minority must include at least four Member States, failing which the qualified majority shall be deemed attained.



February 28, 2017

**Attn:**

Věra Jourová  
Commissioner for Justice, Consumers and Gender Equality  
European Commission

**CC:**

Claude Moraes  
Chairman, Committee on Civil Liberties, Justice and Home Affairs (LIBE)  
European Parliament

Frans Timmermans  
First Vice-President, Better Regulation, Interinstitutional Relations, the Rule of Law and the Charter of Fundamental Rights  
European Commission

Andrus Ansip  
Vice-President, Digital Single Market  
European Commission

Isabelle Falque-Pierrotin  
Chairwoman, Article 29 Working Party  
European Commission

Dear Commissioner Jourová,

Recent developments in the United States call into question assurances by the US government that formed the foundation of both the Privacy Shield agreement and the US-EU umbrella agreement. We write to urge you to reexamine whether these agreements sufficiently protect the fundamental rights of people in the European Union in light of these changed circumstances.

In recent weeks, President Donald Trump has issued several executive orders that represent an attack on the rights of immigrants and foreigners—including specific provisions designed to strip these individuals of critical privacy protections that have been provided by previous Democratic and Republican administrations for decades. Concurrently, there has been a deterioration in existing oversight and accountability structures that impact whether, consistent with the ruling in the *Schrems*<sup>1</sup> and *Digital*

---

<sup>1</sup>Case C-362/14, *Schrems v. Data Protection Comm'r*, 2000 EUR-Lex 520 (Oct. 6, 2015), <http://curia.europa.eu/juris/liste.jsf?td=ALL&language=en&jur=C&parties=Schrems>.

*Rights Ireland* judgments<sup>2</sup>, people in the EU are afforded appropriate privacy protections and redress in cases where their data is transferred to the US.

Previously, the ACLU and other rights organizations have written to you expressing our view that reform to US surveillance laws is necessary to ensure that EU data transferred to the US receives protection that is “essentially equivalent” to the protections required under the EU Charter—calling into question the legality of the existing Privacy Shield agreement (Attachment 1).<sup>3</sup> We have also stressed the inadequacy of existing privacy oversight and redress mechanisms for both US residents and individuals around the world. The following recent changes to US policies only deepen our concerns that assurances underpinning both the Privacy Shield and US-EU umbrella agreement are not valid, requiring a reexamination of whether these agreements are consistent with the rights enshrined in the EU Charter of Fundamental Rights:

- Issuance of the executive order *Enhancing Public Safety in the Interior of the United States*: Issued on January 25, 2017, Section 14 of the executive order reverses policies of the Bush, Obama, and prior administrations by prohibiting federal agencies, consistent with applicable law, from providing Privacy Act protections to individuals who are not US citizens or lawful permanent residents.<sup>4</sup> As a result of this change, people in the EU have diminished protections when it comes to limits on dissemination of their personal information, the right to access their private information held by the US government, and the right to request corrections to their information.
- Deterioration of the Privacy and Civil Liberties Oversight Board (PCLOB): The Privacy and Civil Liberties Oversight Board, while fulfilling a valuable public reporting role, is limited in its oversight function and was not designed to provide redress concerning US surveillance practices. Thus, the PCLOB has never provided remedies for rights violations or functioned as a sufficient mechanism to protect personal data. In recent months, the situation has worsened: the PCLOB currently lacks a quorum, which strips its ability to issue public reports and recommendations, make basic staffing decisions, assist the Ombudsman created by the Privacy Shield framework,

<sup>2</sup> Case C-293/12, *Digital Rights Ireland v. Minister for Comm.*, 2006 EUR-Lex 24 (Apr. 8.

2014), <http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=403885>.

<sup>3</sup> In addition to the concerns outlined in that letter, we note that surveillance conducted under Executive Order (EO) 12,333, also violates the standards articulated by the Court of Justice in *Schrems*. This surveillance, which the US government largely conducts outside US soil, implicates EU citizen communications as they are in transit from the EU to the US. See Eur. Comm’n, Implementing Decision, 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, ¶ 75 (Dec. 7, 2016) available at [http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision\\_en.pdf](http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf). Notably, EO 12,333 is the primary authority under which the NSA conducts foreign intelligence, and it encompasses numerous bulk collection programs that involve acquiring communications on a generalized basis, without discriminants. See, e.g., Letter from ACLU to Privacy and Civil Liberties Oversight Board (Jan. 13, 2016), <https://www.aclu.org/letter/aclu-comments-privacy-and-civil-liberties-oversight-board-its-review-executive-order-12333>. In PPD-28, the US effectively acknowledged and ratified its bulk collection practices under this authority. See Press Release, White House Office of the Press Secretary, Presidential Policy Directive—Signals Intelligence Activities: Presidential Policy Directive/PPD-28 (Jan. 17, 2014), <https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>.

<sup>4</sup> Exec. Order No. 13,768, 82 Fed. Reg. 8,799 (Jan. 25, 2017), available at <https://www.gpo.gov/fdsys/pkg/FR-2017-01-30/pdf/2017-02102.pdf>.



and conduct other routine business as part of its oversight responsibilities.<sup>5</sup> The current administration and Senate have yet to act to fill the vacancies on the PCLOB.<sup>6</sup>

1. Executive order: *Enhancing Public Safety in the Interior of the United States*:

As part of the *Schrems* judgment, the Grand Chamber of the Court of European Justice of the European Union emphasized that Article 7 and 8 of the EU Charter of Fundamental Rights requires:

“...clear and precise rules governing the scope and application of a measure and imposing minimum safeguards so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of their data.”<sup>7</sup>

In addition, they emphasized that any legislation:

“...not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protections, as enshrined in Article 47 of the Charter.”<sup>8</sup>

Consistent with this requirement, the Privacy Shield framework adequacy determination relied in part on US government assurances that there were appropriate mechanisms in place for individuals to seek redress in cases where their data was accessed by the US government.<sup>9</sup> Similarly, the umbrella agreement requires the US to ensure that individuals are entitled to seek access and correction to their personal information, unless specified exceptions apply.<sup>10</sup> The umbrella agreement also requires that the US provide the ability to seek administrative redress to individuals in the EU in cases where they are improperly denied the ability to access or correct their information.<sup>11</sup>

However, provisions in the recent executive order issued by the Trump administration raise concerns regarding whether EU data transferred to the US meets the standards outlined in these documents. Specifically, Section 14 of the executive order states that federal agencies “shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information.” Prior to issuance of the executive order, consistent with a 1975 OMB recommendation, many federal agencies, as a matter of longstanding policy, provided certain Privacy Act protections to databases that contained the information of US persons (defined as US citizens and lawful permanent

---

<sup>5</sup> 50 U.S.C. § 601 note; See also GARRETT HATCH, *PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD: NEW INDEPENDENT AGENCY STATUS* (Cong. Research Service, 2012), <https://fas.org/srg/crs/misc/RL34385.pdf>.

<sup>6</sup> Elisabeth Collins is the only sitting members of the PCLOB and is a member of the Republican party.

<sup>7</sup> *Schrems*, *supra* note 1 at ¶ 91.

<sup>8</sup> *Id.* at ¶ 95.

<sup>9</sup> Comm’n Implementing Decision (EU) No. 2016/1250, 2016 O.J. (L. 207/1) ¶ 25, available at <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D1250&from=EN>.

<sup>10</sup> Agreement Between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses (draft 2016) at articles 16 and 17, available at [http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement\\_en.pdf](http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf).

<sup>11</sup> *Id.* at article 18

residents) and non-US persons.<sup>12</sup> These protections included limits on dissemination without consent (subject to exceptions), the right to access your own agency records, the right to request corrections to your records, and remedies where an agency fails to comply with certain requirements. As a result of Section 14, however, these rights will no longer be fully provided to individuals residing within the EU.

While the Judicial Redress Act provides some additional privacy protections for EU citizens, it does not completely mitigate the impact of the executive order's provision for several reasons. First, the Judicial Redress Act only applies to citizens of EU countries.<sup>13</sup> Thus, if an individual lawfully works or lives in the EU, but has not obtained full citizenship status, then he or she may not be entitled to protection under the Judicial Redress Act. Thus, the EO provision strips privacy protections from thousands of lawful EU immigrants.

Second, the Judicial Redress Act alone does not provide the full range of Privacy Act protections that were provided as a matter of policy, prior to issuance of the executive order.<sup>14</sup> The Judicial Redress Act only extends the right to EU citizens to bring a case in civil court to challenge US government action if their records were "willfully and intentionally" disseminated without consent in violation of relevant provisions of the Privacy Act, or in cases where a "designated federal agency or component" fails to comply with a request for information or correction.<sup>15</sup> Thus, even with the Judicial Redress Act, EU citizens may be left without appropriate recourse to address improper dissemination of their information that is accidental or inadvertent in nature. In addition, EU citizens may be unable to address failures to provide access or corrections in cases where their information is held by federal agencies that are not designated under the bill. For example, the Department of Health and Human Services (HHS) has several databases that contain personal information of refugees and immigrants to the US. However, HHS is not a designated agency under the Judicial Redress Act, and thus EU citizens may not be able to access or request corrections to information held by HHS.<sup>16</sup> Moreover, only information shared with the US government by an entity in a EU country for law enforcement purposes is covered—personal information collected by US agencies themselves is not covered, nor is information collected for non-law enforcement purposes such as intelligence gathering.

Finally, the Judicial Redress Act requires that an individual file a civil claim to enforce their rights, and does not require that federal agencies create an administrative process to address privacy violations. As a practical matter, this means that enforcement of EU citizens' rights may not only be time consuming, but

---

<sup>12</sup> Memorandum from Hugo Teufel III, Chief Privacy Off., DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-US Persons (Jan. 7, 2009), *available at* [https://www.dhs.gov/xlibrary/assets/privacy/privacy\\_policyguide\\_2007-1.pdf](https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf); See Privacy Act of 1974; System of Records Notice, 81 Fed. Reg. 46682 (July 18, 2016), *available at* <https://www.gpo.gov/fdsys/pkg/FR-2016-07-18/pdf/2016-16812.pdf>.

<sup>13</sup> Judicial Redress Act, Pub. L. No., 114-126, §2(f), 130 Stat. 282 (2016), *available at* <https://www.congress.gov/114/plaws/publ126/PLAW-114publ126.pdf>.

<sup>14</sup> It is worth noting that the Privacy Act contains numerous exceptions for national security and law enforcement purposes. As a result, even for individuals in the United States, it does not provide adequate redress opportunities in cases where individuals believe their rights have been violated as a result of surveillance. However, the policy change would eliminate even this limited protection. 5 U.S.C. § 552a.

<sup>15</sup> Judicial Redress Act, *supra* note 12 at § 2(a).

<sup>16</sup> Judicial Redress Act of 2015; Attn'y Gen. Designations, 82 Fed. Reg. 7860 (Jan. 23, 2017), *available at* <https://www.federalregister.gov/documents/2017/01/23/2017-01381/judicial-redress-act-of-2015-attorney-general-designations>.

also costly. Thus, while the Judicial Redress Act provides some relief to EU citizens, it does not fully mitigate the impact of the executive order.

## 2. Privacy and Civil Liberties Oversight Board

The CJEU has emphasized that appropriate oversight is critical to ensuring that EU data receives appropriate privacy and other fundamental rights protections. Thus, as part of its adequacy determination for the Privacy Shield, the European Commission relied on assurances that the US intelligence community was subject to various oversight mechanisms, including the PCLOB. The adequacy determination notes that the PCLOB ensures appropriate oversight over US surveillance practices by examining relevant records, issuing recommendations, hearing testimony, and preparing reports (including an examination of PPD-28).<sup>17</sup> Similarly, supporting documentation provided by the Director of National Intelligence asserted that the PCLOB is an independent oversight body that is part of “robust and multi-layered oversight”.<sup>18</sup>

Even with a fully-functioning PCLOB, we had serious concerns that there was not effective oversight of US surveillance activities, and we strongly disagreed with many of the US government’s assertions in this arena. However, notwithstanding these concerns, it is clear that the European Commission relied on the representations regarding the oversight role of the PCLOB as part of its adequacy determination. Unfortunately, however, the PCLOB is no longer a fully functional body. Currently four of the five board positions on the PCLOB are vacant.<sup>19</sup> Without a quorum, the PCLOB cannot issue reports and recommendations, including its planned report on activities conducted under executive order 12333 and the implementation of PPD-28.<sup>20</sup> In addition, the Board is further limited in its ability to make staffing decisions necessary to fulfill its responsibilities.<sup>21</sup> Moreover, the vacancies also impact the extent to which the Board’s membership represents diverse political viewpoints. Under statute, no more than three of the Board members may come from the same political party, ensuring that a full Board contains representation from both political parties. The current membership, however, represents only one political party.

The process of filling the vacancies on the Board is not an easy one. It requires nomination by the President and confirmation by the Senate—a process that can be lengthy, arduous, and easily derailed. Indeed, the PCLOB remained largely dormant from 2007 to 2012 due in part to these hurdles. For the PCLOB to operate effectively, it is critical that the President appoint and the Senate confirm individuals with a demonstrated commitment to and background in privacy, civil liberties, and transparency.

Given these recent changes to US policies and oversight structures, we believe that the assurances that the European Commission relied on as part of the Privacy Shield and US-EU umbrella agreement are no longer valid. Thus, we urge you to examine whether these agreements are consistent with the protections enshrined in the EU Charter of Fundamental Rights.

---

<sup>17</sup> *Comm’n Implementing Decision*, *supra* note 8 at ¶ 95.

<sup>18</sup> *Id.* at Annex VI.

<sup>19</sup> *Board Member Biographies*, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD (Accessed Feb. 21, 2017), <https://www.pclob.gov/about-us/board.html>.

<sup>20</sup> See also, 6 C.F.R. § 1000.3 (2013), available at <https://www.pclob.gov/library/FederalRegister-PCLOB-2013-0005-Delegation-Reg.pdf>.

<sup>21</sup> *Id.*

Sincerely,



**Faiz Shakir**  
Director  
American Civil Liberties Union



**Lotte Leicht**  
European Union Director  
Human Rights Watch



**Neema Singh Guliani**  
Legislative Counsel  
American Civil Liberties Union



**Cynthia M. Wong**  
Senior Internet Researcher  
Human Rights Watch



**Sarah St. Vincent**  
Researcher, U.S. Division  
Human Rights Watch