Mr. Bruno Gencarelli
Head of Unit for International Data Flows and Protection
European Commission
JUST-C4@ec.europa.eu

5 July 2017

Re: Access Now Responds to Privacy Shield Review Questionnaire

Mr. Gencarelli,

Thank you for your invitation to provide information and observations on the European Commission's review of the EU-U.S. Privacy Shield arrangement. The Privacy Shield is the mechanism to facilitate the processing of the personal data of persons in the European Union within the United States. Because the potential for the global movement of data is at the heart of a free and open internet, the Privacy Shield and other arrangements like it are highly important to providing a rights-respecting internet infrastructure. However these arrangements must comply with international and European human rights law, including on data protection. In order to ensure that this is the case, the European Commission should subject the Privacy Shield and U.S. practices implicating the rights of people in the EU to an exacting review.

Access Now is an international organisation that defends and extends the digital rights of users at risk around the world.[1] By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all.

Access Now maintains presences in 10 locations around the world, including in the policy centers of Washington, DC and Brussels.[2] Access Now has spent many years working on data transfer arrangements under EU law, including the Safe Harbor that was invalidated by the Court of Justice of the European Union in 2015 and now the Privacy Shield as its replacement.[3]

You have specifically asked us to provide feedback on two main areas:

- Relevant developments in the U.S. legal framework (legislative, regulatory, administrative or case-law developments) since August 2016 that you consider to be relevant for compliance by certified U.S. companies with their obligations under the Privacy Shield as well as regards the limitations and safeguards applicable to access by U.S. authorities to personal information transferred from the EU for public interest, in particular law enforcement and national security reasons; and
- Functioning of redress and (administrative and judicial) review mechanisms referred to in the Privacy Shield adequacy decision, both as regards compliance by certified U.S. organisations and government access.

[1] https://www.accessnow.org/.
[2] https://www.accessnow.org/about-us/.
[3] *See* https://www.accessnow.org/tag/eu-us-privacy-shield/.

In addition, you have also asked for our views on the "safeguards applicable to U.S. companies in the area of automated decision-making that may produce legal effects on, or significantly affect the rights/obligations of, consumers, in particular to ensure that they have the possibility to contest such a decision," as well as "any other information relating to the implementation of the Privacy Shield that you would like to bring to the attention of the Commission in preparation of the first annual review."

We will address each request in turn.

I. Developments in U.S. law and policy since August 2016 undermine the human rights of people in the EU

In February 2017, Access Now wrote to Commissioner Jourová and Claude Moraes.[4] We highlighted several developments in the U.S. that we thought significantly impacted the United States' commitments under the Privacy Shield:

- Loss of four members of the Privacy and Civil Liberties Oversight Board ("PCLOB"), a key intelligence oversight agency, at a key time prior to the publication of a report on surveillance of non-U.S. persons;
- Promulgation of an Executive Order that demonstrated a disregard for the rights of any non-Americans;
- Appointment of several individuals who have demonstrated a disregard for human rights to lead U.S. intelligence agencies
- Expansion of Executive Order 12333 to allow the broader distribution of personal data collected under its expansive reach within the intelligence community.

Specifically, we explained,

> "These developments show a near-reckless disregard for the human rights of Europeans and others outside the United States and foreshadow further weakening of the already watered-down protections for Europeans' data."[5]

This statement remains true today. In addition, since February there have been further developments that are worth noting. We'll discuss several of them here.

1. *The continued debate over authorization of expansive U.S. surveillance targeted at non-Americans*

Section 702 of the FISA Amendments Act ("FAA") is the legal authority under which surveillance programs known to the public as "Prism" and "Upstream" are operated.[6] These programs, which are targeted at non-U.S. persons, are exceptionally broad. The law does not require government agents to request surveillance related to specific targets. Instead, the U.S. Attorney

[4] https://www.accessnow.org/cms/assets/uploads/2017/02/Letter-to-Jourova.pdf.
[5] *Id*.
[6] https://www.law.cornell.edu/uscode/text/50/1881a; *see also* https://www.accessnow.org/new-call-u-s-surveillance-reform.

General and the Director of National Intelligence ("DNI") submit to the Foreign Intelligence Surveillance Court ("FISC"), on an annual basis, an application for the approval of surveillance programs that target non-U.S. persons located outside the U.S.[7] "Non-U.S. persons" includes those who are not citizens or permanent residents in the U.S., as well as companies and organizations incorporated outside the United States.[8]

Because of the broad nature of these programs, for anyone outside the United States, the issue is less about how 702 authority is "abused" and more about the inherently privacy-invasive and harmful ways it can permissibly be used.

Section 702 was passed with an expiration date in order to ensure that it was regularly re-examined by Congress. The first sunset was 2012, at which point Congress passed a 5 year "clean" re-authorization - an authorization without any amendments or changes.[9] Currently the law is set to expire on December 31, 2017 unless another extension is passed.

The debate over Section 702 is relevant to the Privacy Shield. The operation of programmes under Section 702 were central to the invalidation of the Safe Harbour by the Court of Justice of the European Union ("CJEU").[10] Further, even though Privacy Shield wasn't, facially, contingent on reforms to Section 702, the Privacy Shield operates under incorrect assumptions about U.S. surveillance.[11] Finally, the debate around Section 702 is the best indicator of the approach that U.S. government officials are taking toward the protection of the rights of people in the EU.

So far, several reform proposals that have been discussed for Section 702.[12] These include:

- Codification of Presidential Policy Directive 28 ("PPD 28"), which recognized for the first time the privacy interests (although not rights) of non-U.S. persons;
- Prohibition of the acquisition of communications that are not to or from targets;[13]

---

[7] *Id*.

[8] https://www.law.cornell.edu/uscode/text/50/1801.

[9] https://www.congress.gov/bill/112th-congress/house-bill/5949/text.

[10] http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=786213.

[11] https://www.accessnow.org/three-facts-us-surveillance-european-commission-gets-wrong-privacy-shield/.

[12] https://www.accessnow.org/new-call-u-s-surveillance-reform/.

[13] It is important to note that in May 2017 the U.S. National Security Agency ("NSA") implemented this change procedurally when it halted its practice of "about" collection — that is, the practice of collecting information not only to or from surveillance targets, but also "about" those targets (meaning the NSA collects the communications of people who are not relevant to an investigation). https://nsa.gov/news-features/press-room/press-releases/2017/nsa-stops-certain-702-activites.shtml. As we have said, this change is actually a "major victory for the human rights of people around the world." https://www.accessnow.org/u-s-stop-spying-without-protecting-human-rights-fixing-section-702-start/. However, the change was not really "voluntary" in that it only came upon pushback from the Foreign Intelligence Surveillance Court about incidental surveillance of U.S. persons. Additionally, reports indicate that even now the Agency is looking for ways to re-start this overbroad collection, making codification of meaningful reforms even more important. https://www.eff.org/deeplinks/2017/06/liveblogging-todays-senate-judiciary-hearing-section-702 ("The NSA's Paul Morris told Feinstein that the NSA would like to

- Limitation of surveillance to exclusively target foreign powers or agents of foreign powers.

Several major internet companies recently joined the chorus of human rights and U.S. civil liberties organizations pushing for reforms, calling on Congress to implement a number of changes to Section 702.[14]

We believe that, *if codified*,[15] the Section 702 reforms supported broadly by civil society and the corporate sector — substantive changes accompanied by increased transparency and oversight and a new sunset date — represent the significant first step in the reform process needed to drive the Privacy Shield arrangement through at least this initial review, though only if it comes with a commitment for continued meaningful engagement on further surveillance reforms.[16]

However, despite this emphasis on reform, on June 6, 2017, fourteen senators introduced a bill in Congress that not only would permanently reauthorize the FAA, but would expand other U.S. surveillance authorities.[17] The bill will also roll back the USA FREEDOM Act, a key surveillance reform implemented in 2015 that was oft-cited in the negotiations over the Privacy Shield.[18] While it does not yet have broad support in Congress, officials from the intelligence community have offered their support for reauthorization without further sunset.[19] The presence of this bill will undoubtedly influence of Congressional conversations about reform, and it demonstrates a broadly held opinion in Congress that non-U.S. persons, including people in the EU, do not and should not have cognizable human rights protections.

2. *The Foreign Intelligence Surveillance Court (FISC) has provided evidence of willful mis-use of authorities*

It is true as we said above that one of the major problems with U.S. surveillance authorities directed extraterritorially, including at people in the EU, is not how they are abused but the scope of their legitimate use. However, the issue of potential abuse was central to negotiations over Privacy Shield and as such remains relevant to this discussion. In his letter to U.S. officials in support of the Privacy Shield, Robert Litt, who was then-General Counsel of the Office of the Director of National Intelligence (ODNI), stated:

> "The Department of Justice and the ODNI closely review and scrutinize the use of Section 702 to verify compliance with legal rules; agencies are also under an

---

keep open the possibility of restarting about collection if they can find a technical solution that minimizes the amount of unnecessary information about Americans obtained through about collection.").

[14] http://www.ccianet.org/wp-content/uploads/2017/05/702-letter-201705-FINAL.pdf.

[15] https://www.accessnow.org/cms/assets/uploads/2017/05/FISA702.HJC_.pdf.

[16] https://www.accessnow.org/u-s-stop-spying-without-protecting-human-rights-fixing-section-702-start/.

[17] https://www.accessnow.org/ahead-702-hearing-u-s-senators-push-make-control-spying-powers-permanent/.

[18] https://www.cotton.senate.gov/?p=press_release&id=693.

[19] https://www.eff.org/deeplinks/2017/06/liveblogging-todays-senate-judiciary-hearing-section-702 ("Sen. Amy Klobuchar pushed back on the intelligence officials' testimony that Section 702 should be reauthorized without a sunset. That would give Congress "no leverage to get changes or to work on things," she said, noting that Sen. Feinstein—who has historically defended the intelligence community—said she would oppose reauthorization without a sunset.").

> independent obligation to report potential incidents of noncompliance. Those incidents are investigated, and all compliance incidents arc reported to the Foreign Intelligence Surveillance Court, the President's Intelligence Oversight Board, and Congress, and remedied as appropriate. ***To date, there have been no incidents of willful attempts to violate the law or circumvent legal requirements.***"[20]

However, even as privacy experts have continually debated his assertion that there had been no "willful attempts to violate [Section 702]," today it is inarguably no longer the case. As noted by independent reporter Marcy Wheeler:

> "The Intelligence Committees started requiring copies of all interagency IC related MOUs last year...Nevertheless, that doesn't change the history, that FBI at an institutional level made a decision to provide (apparently small amounts of) data to people outside of the minimization procedures."[21]

This represents a meaningful change in the circumstances as they were when Privacy Shield negotiations were concluded. However, it is unclear if the U.S. has communicated this change to the Commission. In fact, during recent testimony given after these abuses were published, government officials repeated Mr. Litt's assertion about the lack of willful violations of Section 702.[22] This misrepresentation casts wide doubt on all such assertions by U.S. intelligence officials.

3. *The intelligence community has abruptly abandoned its multi-year promise to provide necessary transparency into surveillance programs*

In his confirmation hearings in February 2017, the current DNI, Dan Coats, re-committed to providing an estimate of the number of U.S. Persons which have had their communications incidentally collected under Section 702. He recognized that there had been a long promise to provide such information and said "I will do everything I can...to get you that number."[23] In fact, members of Congress have been asking for this estimate since 2011,[24] and civil society has made it a priority since at least 2015.[25]

---

[20] http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-6_en.pdf. Internal citations omitted. Emphasis added.
[21] https://www.emptywheel.net/2017/06/27/the-willful-fbi-702-violation-no-one-admitted/.
[22] https://www.judiciary.senate.gov/imo/media/doc/06-27-17%20Brooker-Evans-Morris-Ghattas%20Joint%20Testimony.pdf. ("Using the reviews by DOJ and ODNI personnel, the Attorney General and the DNI assess semiannually, as required by Section 702, compliance with the targeting and minimization procedures and the acquisition guidelines. These assessments, which have been regularly produced to this Committee since the inception of the FAA, conclude that the number of compliance incidents has been small relative to the scope of collection, with *no indication of any intentional attempt to violate or circumvent any legal requirements*.) (emphasis added).
[23] https://www.c-span.org/video/?424444-1/former-senator-dan-coats-testifies-dni-confirmation-hearing. *See also* https://www.scribd.com/document/295340256/ODNI-Reply-to-NGO-Letter-Regarding-702-Transparency.
[24] https://www.wyden.senate.gov/download/?id=351e298f-134c-4a24-9128- e61f5aa54727&download=1.
[25] *See, e.g.*, https://na-production.s3.amazonaws.com/documents/CoatsResponseLetter_6_12.pdf.

However, despite multiple commitments to provide this number, in a June 2017 Congressional hearing, with no advance warning, Director Coats affirmatively disavowed his commitment and indicated that the Department would no longer pursue the requested estimate.[26]

In our official reaction to Director Coats announcement we asserted:

> "Director Coats' reversal on this important issue is significantly troubling for transparency and accountability. Section 702 authorizes global surveillance that undermines the right to privacy of people in the U.S. and around the world. Giving information on the U.S. persons implicated by this authority would not have provided adequate transparency on its full reach. However, it was a vitally important step toward getting the information we need to understand how the programs impact people and their personal data. Now, rather than taking a first step forward, we are leaping backward. Refusing to honor that pledge backtracks on the transparency that the intelligence community has continually promised to provide after revelations that these programs are overbroad, and it shows profound disrespect for the people to whom those promises were made, in the U.S. and elsewhere."[27]

People in the EU cannot expect to gain the necessary transparency into the impact of U.S. surveillance upon their own personal information when the DNI treats his commitments to U.S. persons with such casual disregard.

4. *The U.S. is not adequately protecting the rights of people in the EU as against MLAT bypass agreements currently being pursued, particularly by the UK*

The U.S. government has been working to amend domestic law to permit officials from other governments to bypass the Mutual Legal Assistance Treaty ("MLAT") process. Under the proposed statutory change, which would amend the Electronic Communications Privacy Act ("ECPA"), permission to issue direct requests for user data to U.S. companies would be allowed under reciprocal bilateral agreements with the U.S. government. The United Kingdom is already pursuing such an agreement and, along with U.S. officials, has been actively pushing for the necessary change in ECPA to allow for the agreements.[28]

The proposed amendment to ECPA contains some language on human rights, but it is not strong enough to offer meaningful protections, particularly to non-U.S. persons: it only requires a limited human rights certification for participating countries.[29] If the U.S. is to adequately

---

[26] *Id.*

[27] https://www.accessnow.org/coalition-u-s-intelligence-director-no-backtracking-surveillance-transparency/.

[28] https://www.documentcloud.org/documents/2994379-2016-7-15-US-UK-Biden-With-Enclosures.html#document/p4; *see also* https://judiciary.house.gov/wp-content/uploads/2017/06/Downing-Testimony.pdf (page 13); https://judiciary.house.gov/wp-content/uploads/2017/06/McGuinness-Testimony.pdf (page 3).

[29] https://www.accessnow.org/diagnosis-current-proposals-fix-mlat-system-wont-work/. In addition to the limited human rights protections being considered for ECPA, only the domestic protections afforded by a

protect the human rights of persons in the EU under this proposed agreement, any change to ECPA must come with much-strengthened human rights protections.

If additional human rights protections are not required, any resulting agreement with the UK, if and when entered into, will greatly expand the reach of invasive UK surveillance authorities vis a vis individuals around the world, including people in the EU. Right now, the UK is implementing the newly-promulgated Investigatory Powers Act ("IP Act") while also negotiating its exit from the European Union. While the Brexit negotiations will not relieve the UK of its obligations under the EU Charter for Fundamental Rights or the European Convention on Human Rights, the IP Act and its grant of broad authority to conduct bulk surveillance on persons outside the UK demonstrates that the UK already does not respect these human rights commitments.[30] Further, there is a growing possibility that the UK will take further actions against human rights as it pursues its departure from the European Union. In fact, Prime Minister Theresa May recently made clear her disdain for human rights protections: "if human rights laws get in the way of tackling extremism and terrorism, we will change those laws to keep British people safe."[31] This trend away from respect for human rights in the UK, combined with a broader reach for UK surveillance into the U.S., will further undermine the rights of people in the EU.

II. Privacy Shield redress mechanisms are inadequate to protect EU persons

As emphasized by the Article 29 Working Party ("WP29"), "effective remedies need to be available to the individual: anyone should have the right to defend her/his rights before an independent body."[32] However, the redress mechanisms implemented by and for Privacy Shield fail to provide users effective, meaningful, or transparent access to remedy. There are two primary redress mechanisms: (1) those created to provide access to public authorities for misuses of data collected for law enforcement, national security, or other public interests purposes and (2) those created to address violations of consumer protections provided within the Privacy Shield. We will address each in turn.

1. *The failure of redress mechanisms for law enforcement, national security, and other public interest purposes*

The Privacy Shield created a new redress mechanism - the Privacy Shield Ombudsperson - specifically to address issues of inappropriate state access to user data. According to the European Commission:

---

country made party to a bilateral agreement would apply when that country attempts to access the personal data of people in the EU.

[30] https://www.csmonitor.com/World/Passcode/2016/0112/Opinion-Britain-can-t-pwn-the-world.

[31] https://twitter.com/theresa_may/status/872181737933217794?ref_src=twsrc%5Etfw&ref_url=http%3A%2F%2Fwww.cnn.com%2F2017%2F06%2F07%2Feurope%2Ftheresa-may-terrorism-human-rights%2Findex.html.

[32] http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf.

> "The Privacy Shield Ombudsperson is a senior official within the U.S. Department of State who is independent from U.S. intelligence agencies. Assisted by a number of staff, the Ombudsperson will ensure that complaints are properly investigated and addressed in a timely manner, and that you receive confirmation that the relevant U.S. laws have been complied with or, if the laws have been violated, the situation has been remedied."[33]

The Privacy Shield specifically explains that the arrangement would be suspended, amended, or repealed if the Ombudsperson mechanism was found to have failed. This gives the Ombudsperson central weight in the continued viability of the Privacy Shield.[34]

In fact, the Ombudsperson has not lived up to its promise. Because of this, the position has frequently been criticized by WP29, most recently concerning the transparency and availability of the mechanism.[35] Essentially, the Ombudsperson mechanism is inadequate to provide protection that is essentially equivalent to that prescribed by EU law.

The Ombudsperson mechanism is not adequately independent - As we have articulated previously, the location of the Ombudsperson mechanism under the Secretary of State cannot be considered adequately independent from the intelligence community and free from "improper influence."[36] This opinion has been echoed by Emily O'Reilly, the European Ombudsman.[37] In a letter to the Commission, she emphasized that representing the Privacy Shield Ombudsperson as an independent body might undermine the credibility and trust in the Ombudsperson "as an instrument of democratic accountability." The Privacy Shield does not provide safeguards or details on how the independence of the intelligence community may be guaranteed. This structure does not meet the CJEU's requirements for the independence and impartiality of the oversight and redress mechanism.[38] The Ombudsperson mechanism calls for cooperation between the Ombudsperson and other institutions such as PCLOB and Inspectors General, however the potential independence of these other institutions do not fix the lack of independence of the Ombudsperson itself. Finally, the Ombudsperson position is a political appointment subject to presidential discretion (with the confirmation of the U.S. Senate). A person in this role can be terminated at any time without a cause or obligation to substantiate the decision.

---

[33] http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_en.pdf.
[34] http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf ("Commission will present draft measures [...] with a view to suspending, amending or repealing this Decision or limiting its scope, among others, where there are indications of a systematic failure by the Privacy Shield Ombudsperson to provide timely and appropriate responses to requests from EU data subjects.").
[35] ec.europa.eu/newsroom/document.cfm?doc_id=45272 ("the WP29 stresses the need to obtain information concerning the nomination of the four missing members of the PCLOB as well as on the appointment of the Ombudsperson and the procedures governing the Ombudsperson mechanism, as they are key elements of the oversight architecture of the Privacy Shield.").
[36] *See*, https://www.accessnow.org/three-facts-us-surveillance-european-commission-gets-wrong-privacy-shield/.
[37] https://www.ombudsman.europa.eu/resources/otherdocument.faces/en/64157/html.bookmark.
[38] C-288/12, C-518/07, C-614/10, C-362/14.

The Ombudsperson mechanism lacks investigatory powers - The Privacy Shield claims that "the Ombudsperson mechanism provides for independent oversight with investigatory powers."[39] The recital purposefully refers to the mechanism, which is a procedure that is built on the coordination role of the Ombudsperson and other governmental bodies and officials, and not the Ombudsperson itself. However, Ombudsperson's role is limited and does not entail investigatory powers.[40] Instead, the Ombudsperson merely coordinates complaints and facilitates receipt of information from other government officials, agencies, and independent authorities. Even its notification role is very limited. At the end of the process the Privacy Shield Ombudsperson "confirms compliance or remediation of any non-compliance,"[41] but does not notify the individual if he or she was subject to surveillance or what remedy was applied (if any). This limitation lacks important specificity. The Ombudsperson has no legal powers to enforce the rights of people in the EU as against the U.S. government. Additionally, the Ombudsperson is very dependent on the powers and activities of PCLOB.[42] As we are in the absence of an operating PCLOB the role and efficacy of the Ombudsperson is rendered mostly symbolic.

The Ombudsperson mechanism was absent for several months leaving the position in a state of uncertainty - Under the Obama Administration, the Under Secretary of State for Economic Growth, Energy and the Environment was appointed to the role of Privacy Shield Ombudsperson.[43] Upon the change in administration in January 2017, the position was left vacant. Only in April 2017 did the Department of State website publish that Judith Garber, Acting Assistant Secretary for Oceans, Environment, and Science (OES), was named to the role (the publication was backdated to January 2017).[44] However, the status of Acting Assistant Secretary Garber remains tenuous as she is only filling in the role and is not a confirmed appointee.[45] Additionally, even if and when the position is permanently filled, nothing prevents another prolonged term of absence in the future if the next appointee chooses to leave his or her position. In fact, the current absence sets a troubling precedent against having the role permanently filled.

Beyond the Ombudsperson Mechanism, the Privacy Shield outlines three areas in which the U.S. system provides for some redress mechanisms also available that are also available to people in the EU. Those three areas are (1) interference under FISA; (2) unlawful, intentional access to personal data by government officials; (3) and access to information under Freedom of Information Act.[46] However, these redress options are limited:

---

[39] Recital 124 of the Privacy Shield, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.207.01.0001.01.ENG&toc=OJ:L:2016:207:FULL.
[40] Recital 124 of the Privacy Shield, *Id*.
[41] Recital 124 of the Privacy Shield, *Id*.
[42] Recital 124 of the Privacy Shield, *Id*.
[43] https://iapp.org/news/a/privacy-shield-details-released/; *see also* https://www.theguardian.com/profile/catherine-a-novelli.
[44] https://www.state.gov/e/privacyshield/ombud/.
[45] *See* https://techcrunch.com/2017/04/06/eu-us-privacy-shield-remains-precariously-placed/; https://www.theregister.co.uk/2017/04/12/us_privacy_shield_ombudsman/.
[46] Recital 124 of the Privacy Shield, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.207.01.0001.01.ENG&toc=OJ:L:2016:207:FULL.

"While individuals, including EU data subjects, therefore have a number of avenues of redress when they have been the subject of unlawful (electronic) surveillance for national security purposes, it is equally clear that at least some legal bases that U.S. intelligence authorities may use (e.g. E.O. 12333) are not covered. Moreover, even where judicial redress possibilities in principle do exist for non-U.S. persons, such as for surveillance under FISA, the available causes of action are limited and claims brought by individuals (including U.S. persons) will be declared inadmissible where they cannot show 'standing', which restricts access to ordinary courts."[47]

2. *The failure of redress mechanisms for violating the Privacy Shield Principles*

The Privacy Shield includes a set of rules on enforcement that on principle prescribes that "effective privacy protection must include robust mechanisms for assuring compliance with the Principles."[48] The Privacy Shield then provides for several avenues for redress:

- A complaint filed directly with a company that has self-certified under the Privacy Shield, triggering a duty to respond within 45 days;
- A complaint filed with an "independent" dispute resolution body paid for and chosen by the company.
- A complaint filed with the national Data Protection Authority ("DPA"), which will refer the matter to a dispute resolution body (or panel). The panel issues an advice within 60 days and if the company does not comply with it, the panel can refer the issue either to the U.S. Federal Trade Commission ("FTC") or the U.S. Department of Commerce. The outcome of this process might be the company's removal from the Privacy Shield list but not an individual redress.
- A complaint filed with the DPA, who then cooperates with the FTC and the U.S. Department of Commerce to achieve a resolution within 90 days, though the resolution may be limited by the extent the company chooses to submit to the oversight of the DPA;
- The operation of the FTC's authority to "ensure compliance with the Principles." However, FTC's enforcement has historically been limited to procedural requirements rather than investigating privacy and data protection practices of companies.[49]
- Binding arbitration by the "Privacy Shield Panel." This final redress mechanism is characterized as "last resort," meaning it can only be invoked once all the previous options have failed, although in fact is the first level of a reliable enforceable decision.[50]

[47] Recital 124, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0131+0+DOC+PDF+V0//EN.
[48] Recourse, enforcement and liability of the Privacy Shield Principles, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.207.01.0001.01.ENG&toc=OJ:L:2016:207:FULL.
[49] https://iapp.org/media/pdf/resource_center/IAPP_FTC_SH-enforcement.pdf ("In most cases, however, the Safe Harbor violations alleged by the FTC were "technical" in nature, meaning they were related to the administrative procedures of the Safe Harbor and dealt with the mechanics of certification or recertification, as opposed to enforcement of substantive data principles.").
[50] Recitals 56-58, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.207.01.0001.01.ENG&toc=OJ:L:2016:207:FULL.

Even with a range of redress mechanisms, people cannot meaningfully exercise their rights and reach an enforceable decision unless they go through almost all these six avenues to reach the Privacy Shield Panel.[51] This process is lengthy, opaque, and prevents people in the EU from exercising their rights within the United States.[52]

These Privacy Shield redress mechanisms are not essentially equivalent to what is available for people in the European Union. In the EU, every member state has its own national data protection authority, commissioner, or ombudsperson tasked with enforcing the fundamental rights of privacy and data protection. The enforcement includes ex officio investigations and individual complaints with the possibility of judicial oversight and redress.

In contrast, the available avenues under Privacy Shield are dependent on mostly unenforceable self-regulation. Instead of concrete remedies, like fines, compensation for the individual, or an order for a change in corporate practice, the most likely outcome of pursuit of redress under Privacy Shield is, at most, the removal of a company from the Privacy Shield. DPAs also have an independent right to order suspension of data transfers by a company when, upon receiving a claim by an EU data subject, the DPA considers that a company is in violation of EU data protection law or the Privacy Shield. These options should be exercised at times as the best option to protect the rights of users, regardless of possible economic harm. Suspension of data flow is not a desirable outcome for either businesses or users, therefore companies have a duty as well as an economic interest in facilitating the free flow of data in a right-respecting manner.

There are also barriers to the pursuit of even these limited mechanisms. The general knowledge around data protection enforcement might not be perfect, but Europeans are increasingly aware of the procedures of data protection authorities in case of similar violations within the national and EU context. By contrast, under Privacy Shield people are not notified about the processing of their personal data in the U.S., let alone possible violations and avenues for redress.

Finally, in addition to the six redress mechanisms in Privacy Shield, people may also file litigation or administrative complaints based on "tort law and in cases of fraudulent misrepresentation, unfair or deceptive acts or practices, or breach of contract." However, these avenues do not meaningfully change the above assessment, particularly since pursuit of these mechanisms can often be costly and confusing in an unfamiliar jurisdiction.

III. Additional information that the European Commission may find useful

1. *Other legal and policy developments that implicate privacy and the treatment of the rights of non-U.S. persons in the United States*

In addition to the information detailed above, there have been several other developments in U.S. law and policy that more generally undermine the right to privacy of people in the EU within

[51] Recital 56, *Id*.
[52] https://free-group.eu/2016/04/06/eu-us-privacy-shield-towards-a-new-schrems-2-0-case/.

the United States as well as the general treatment of non-U.S. persons. Here we detail four of those developments.

President Trump's threat that the United States may leave the UN Human Rights Council - In June 2017, Nikki Haley, the U.S. Ambassador to the United Nations, gave a speech in which she hinted that the U.S. may pull out of the UN Human Rights Council. She said, the U.S. is "looking carefully at this council and our participation in it. We see some areas for significant strengthening."[53] This threat casts serious doubts on the commitments the United States has made to human rights globally.

The repeal of the Federal Communications Commission's rule on broadband privacy - In 2016, after a rigorous process and months of public input, the U.S. Federal Communications Commission ("FCC") promulgated rules to empower individuals to decide whether broadband service providers can share sensitive data with other companies, and provide an opt-out for other uses. These standards were not only important for people in the U.S. but sent a global signal that companies must respect users' privacy and safeguard their security. However, in early 2017 Congress voted to repeal these rules in full, an action taken with full Presidential support. By repealing these rules, the U.S. has failed to ensure the protection for user data from some of the biggest threats to their privacy and security online. More importantly, the U.S. now stands at odds with the EU in its ongoing consideration of reforms to the e-Privacy directive.

Changes to the treatment of visitors and travellers to the United States - On February 7, 2017, U.S. Department of Homeland Security Secretary John Kelly told members of the U.S. Congress that his agency was considering a wide range of "extreme vetting" procedures, including requiring that visa applicants provide the U.S. government with the passwords to their social media accounts.[54] Despite widespread opposition to this and other proposals,[55] the U.S. State Department forged ahead to implement several "extreme vetting" practices in May 2017, including "social media handles, phone numbers and emails for the last five years, prior passport numbers and additional information about their family, past travel and employment."[56] At the same time, the U.S. Supreme Court ("SCOTUS") has allowed the implementation of at least part of President Trump's "travel ban" of visitors from certain Muslim-majority countries while considering the full scope of the ban for its final judgment.[57] In addition, there has been a marked increase in the number of instances where border officials are ordering travelers to

[53] http://www.npr.org/sections/thetwo-way/2017/06/06/531752892/trump-administration-warns-that-u-s-may-pull-out-of-u-n-human-rights-council, *cf.* https://www.nytimes.com/2017/06/06/world/europe/united-nations-trump-human-rights.html.
[54] http://www.nbcnews.com/news/us-news/us-visitors-may-have-hand-over-social-media-passwords-kelly-n718216.
[55] https://www.accessnow.org/no-passwords-u-s-border-says-new-fly-dont-spy-coalition/.
[56] https://www.federalregister.gov/documents/2017/05/04/2017-08975/notice-of-information-collection-under-omb-emergency-review-supplemental-questions-for-visa.
[57] http://www.npr.org/2017/06/28/534760203/trump-travel-ban-could-be-implemented-thursday.

"unlock" their devices and give broad access.[58] Finally, the Administration has also implemented a "device ban" for any electronic device "larger than a cell phone or smart phone" in the cabin of flights from certain airports.[59] Reports indicate that officials are looking to expand this ban to include more airports and to also prohibit devices in checked luggage as well.[60]

U.S. Supreme Court's acceptance of *Carpenter v. United States* - In June 2017, SCOTUS agreed to hear *Carpenter v. United States*.[61] In the case, the government applied for and received an order under the U.S. Stored Communications Act to retrieve more than five months of cell phone location records for several phone numbers from various wireless providers.[62] SCOTUS had previously held that a person did not have a privacy interest in information, like location data, that was voluntarily shared with a third-party, like a telephone provider, what is known as the "third party doctrine."[63] That case, however, dealt with very limited data. Then in 2012, SCOTUS found a privacy violation in the attachment and use of a GPS device on a suspect's car to track location over a month.[64] While the opinion rested on the device's physical attachment, several Justices evinced an understanding that access to data over a period of time, even data possessed by a third party, could constitute a privacy invasion. It is possible that *Carpenter* will ultimately decide this question, which would be a major development in U.S. privacy law and doctrine that could influence the scope of United States privacy protections.

2. *Implementation of the EU General Data Protection Regulation*

On May 25, 2018, the General Data Protection Regulation ("GDPR"), including updated data protection rights for users and new rules on the transfer of personal data, becomes applicable. The GDPR replaces the Data Protection Directive 95/46/EC as the legal basis of all adequacy decisions currently in place between the EU and other countries, including the Privacy Shield.

As the GDPR becomes applicable, it is important to ensure that the Privacy Shield is equipped to protect the rights of persons in the EU. In particular, it will become increasingly important to:

- Ensure the principle of purpose limitation is guaranteed by the Privacy Shield

The principle of purpose limitation is including in the Privacy Shield while not being specifically defined.[65] The lack of definition means there are no criteria limiting the scope of collection and

[58] http://thehill.com/policy/cybersecurity/323763-border-agents-demanded-searches-of-us-citizens-phones-nbc-investigation; https://www.nytimes.com/2017/02/14/business/border-enforcement-airport-phones.html.
[59] https://www.dhs.gov/news/2017/03/21/qa-aviation-security-enhancements-select-last-point-departure-airports-commercial. There is little guidance given on what size is considered "larger than a smartphone."
[60] http://www.politico.com/story/2017/06/28/trump-laptop-ban-airlines-worldwide-240056.
[61] http://www.scotusblog.com/case-files/cases/carpenter-v-united-states-2/.
[62] https://epic.org/amicus/location/carpenter/.
[63] http://caselaw.findlaw.com/us-supreme-court/442/735.html.
[64] https://epic.org/amicus/jones/.
[65] Point 5 of the Privacy Shield Principles.

use of personal information as is provided in the GDPR.[66] Furthermore, while both the Privacy Shield and the GDPR foresee the possibility of further processing of personal data, wherein a change of purpose could occur,[67] the GDPR does so subject to a series of safeguards to limit negative impact on users' fundamental rights. The Privacy Shield contains no such safeguards.

- Define user consent as an "affirmative act establishing a freely given, specific, informed and unambiguous indication"

While the GDPR requires an affirmative opt-in to data processing, the Privacy Shield instead provides for an opt-out mechanism, specifically in regard to the distribution of user data to third parties and for expansions in the uses of the data beyond why it was initially collected.[68] The concept of opt-out is intrinsically different to "consent" as defined under the GDPR: it requires no affirmative action. Furthermore, the Privacy Shield provides only that users shall "have the opportunity" to opt-out without any obligation for the company to notify the user about this choice or make the process of opt-out either usable or accessible. It also means that users might not be able to control the use of their personal data in all circumstances. For instance, if a company was to use data for a different, but similar, purpose than the one collected, users will likely not have knowledge of this change let alone the possibility to object to it.

- Guarantee that users can exercise their right to object to automated decision making, including profiling.

The GDPR provides for an extended right to object, which includes the right for users to not be subject to a decision based solely on automated processing, including profiling.[69] The Privacy Shield does not indicate what mechanism is available under which this right could be exercised, either in the context of "regular" processing of data or automated decision making. The right to object simply does not exist under U.S. law and is not provided for under the Privacy Shield. This means that, as opposed to the EU, automated decision processing, including profiling, can (and does) take place in the United States largely without limitation.[70] The difference in

---

[66] Article 5.1.b of of Privacy Shield, Article 6.4 of the GDPR.
[67] Point 5a on Data Integrity and Purpose Limitation of Privacy Shield, Article 6.4 of the GDPR.
[68] Privacy Shield Principles Point 2a on Choice; Article 4.11 of the GDPR.
[69] Article 22 of the GDPR.
[70] As an example, the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act (FACTA) provide the basis of the rules applicable for credit rating. *See* https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/fair-credit-reporting-act; https://www.gpo.gov/fdsys/pkg/PLAW-108publ159/pdf/PLAW-108publ159.pdf. Credit ratings are an evaluation of the risk of prospective debtors failing to pay back a debt. Credit rating agencies conduct this evaluation based on personal information both provided directly by the prospective debtor and through information acquired through third party. The FCRA was developed to safeguard users against credit rating abuses, for instance by allowing user to contest mistakes in their credit ratings. https://epic.org/privacy/fcra/. The FCRA and FACTA however only offer limited opt-out of certain practices such as the sharing of their credit rating with third parties or "pre-screening", which is a practice of using or selling user information for unsolicited offers of credit. It is almost impossible for a U.S. person to open a bank account, get a loan or rent an apartment without a credit score. https://www.theguardian.com/money/2013/nov/10/no-credit-card-score. The FCRA and FACTA conform with U.S. law generally on automated decision with opt-out of further sharing of their profile or to access

approaches mean U.S. companies may incidentally be subjecting personal information of EU data subjects to the same automated decision making process as to U.S. data. This approach appears inherently opposed to the one chosen by the EU in the GDPR whereby users can object to decisions based solely on automated decision making.

Conclusion

Thank you again for the opportunity to provide feedback to this very important inquiry. In light of the above information, we offer the following recommendations on ways to proceed with your review:

- Support and work with the U.S. Congress and relevant stakeholders to promote the implementation of meaningful reforms to Section 702 to increase respect for the human rights of people in the EU, particularly in regard to transparency, including transparency for violations of law and policy, contingent on the continued renewal of the Privacy Shield.
- Support and work with the U.S. Congress and relevant stakeholders to promote stronger human rights language in the proposed amendment to the U.S. Electronic Communications Privacy Act.
- Amend the Privacy Shield to include effective individual redress mechanisms and independent oversight and invest in better promoting those mechanisms and raise awareness for people in the EU in how to pursue them.
- In collaboration with the Article 29 Working Party, conduct a separate review the Privacy Shield as well as all other adequacy decisions to ensure compliance of adequacy decisions with the GDPR, ahead of May 25, 2018. In particular:
    - Ensure that the principle of purpose limitation is adequately defined,
    - Define user consent as an "affirmative act establishing a freely given, specific, informed and unambiguous indication", and
    - Guarantee that users can exercise their right to object to automated decision making, including profiling.
- Review the cooperation between the DPAs and the FTC under the Privacy Shield in light of the establishment of the European Data Protection Board and the GDPR.[71]
- Ensure the meaningful participation of WP29, as well as the European Parliament and civil society, in the Privacy Shield review process.
- Commit publicly to transparency by publishing all relevant documents, working papers, and findings from the Privacy Shield review process.

---

information but rarely provides for the possibility for users to "object", or even opt-out, of profiling as a whole. Opt-out is not an appropriate mechanism to obtain user approval for automated decision making. Opt-out mechanisms typically suffer from cumbersome processes, offer little notice or explanation on the nature of the use, and often even deliberately obfuscate the methods and purposes of use of personal information. Moreover, the possibility to opt-out is often meaningless in situations where users have no context to understand how a service can impacts their privacy.

[71] Chapter VII of the GDPR.

If you have any additional questions or would like more information on any of the points we raise in this comment, you can contact our policy experts below. We look forward to the results of your review.

Sincerely,

Amie Stepanovich
U.S. Policy Manager
amie@accessnow.org

Fanny Hidvegi
European Policy Manager
fanny@accessnow.org

Drew Mitnick
Policy Counsel
drew@accessnow.org

Estelle Massé
Senior Policy Analyst
estelle@accessnow.org