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

15 August 2018

Re: Access Now Responds to Privacy Shield Second Annual Review Questionnaire

Mr. Gencarelli,

Thank you for your invitation to provide information and observations on the European Commission's second annual review of the EU-U.S. Privacy Shield arrangement, the mechanism to facilitate the transfer and processing of the personal data of individuals in the European Union within the United States.

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 eleven cities around the world, including in the policy centers of Washington, DC and Brussels.[2]

Access Now has spent many years working to improve data transfer arrangements under EU law, including the Safe Harbor that was invalidated by the Court of Justice of the European Union (CJEU) in 2015 and now the Privacy Shield as its replacement.[3] In February 2017, Access Now wrote to Justice Commissioner Věra Jourová and LIBE Chair Claude Moraes to highlight several developments that significantly impacted the United States' commitments under the Privacy Shield.[4] Later that year, Access Now provided information on the Commission's first review of the Privacy Shield.[5] In our response, we noted that the Privacy Shield and other arrangements like it are highly important and must comply with international and European human rights law, including on data protection. Accordingly, we called for the Commission to subject the Privacy Shield and U.S. practices implicating the rights of individuals in the EU to an exacting review and offered several recommendations.

In 2018, the situation for the Privacy Shield has only deteriorated. In the past year we have seen serious expansions in U.S. surveillance law. Additionally, prominent controversies like the use of Facebook-held data by Cambridge Analytica underscore the limitations of the U.S. Federal Trade Commission (FTC) as a data protection authority.

[1] https://www.accessnow.org/.
[2] https://www.accessnow.org/about-us/.
[3] https://www.accessnow.org/tag/eu-us-privacy-shield/.
[4] https://www.accessnow.org/cms/assets/uploads/2017/02/Letter-to-Jourova.pdf.
[5] https://www.accessnow.org/cms/assets/uploads/2017/07/AN-PSReviewResponse-1.pdf.

We appreciate the difficult position of the European Commission. On one hand, the continued viability of the Privacy Shield rests largely on the scope and implementation of U.S. law, which the Commission cannot control or change. On the other hand, the Privacy Shield is an important economic instrument that facilitates transatlantic business and, as such, the Commission is incentivised to perpetuate its existence. While this may be the reality, the Commission cannot allow the United States to continue to undermine the human rights of Europeans without consequence. The Privacy Shield had the potential to act as an important lever to protect against abusive practices in the United States. However, the U.S. Congress and the Executive have continuously ignored or consciously disregarded the provisions of the Privacy Shield and the facts of the underlying court case that precipitated its existence. These acts, or lack thereof, necessitate a reflection on how much more (or less) the United States have to do to cause the vacation of the arrangement and how much longer can the EU Commission tolerate this situation. Under the circumstances detailed in our submission, maintaining Privacy Shield in its current form does not provide for legal certainty. We urge the Commission to take action for the protection of EU data subjects rights and to suspend the arrangement. .

It is in this spirit that we answer the Commission's request. For the Commission's second review, you have asked for feedback in four primary areas:

1. **Recent developments in the U.S. legal framework;**
2. **Compliance monitoring and enforcement;**
3. **Functioning of redress and review mechanisms; and**
4. **Automated decision-making.**

We will start by analysing further developments in the areas we identified in the first review in 2017. We will then address each of the topics put before us in turn.

### *0. Progress on 2017 Developments*

In Access Now's submission to the Commission's 2017 review we raised several developments in United States law and policy that weighed on the continued viability of the Privacy Shield. Many of these shortcomings remain outstanding, and in fact many have been exacerbated in the intervening period. Here we reiterate these points and provide brief updates on their current status.

- *The loss of four members of the Privacy and Civil Liberties Oversight Board (PCLOB), a key intelligence oversight agency*

The PCLOB has sat with only a single member since February 2017. In September 2017, President Trump nominated Adam Klein to take over as the new Chairman of PCLOB.[6] The

[6] https://www.congress.gov/nomination/115th-congress/929.

announcement was met with sharp criticism given that Klein has vocally supported warrantless surveillance and opposed meaningful reforms to U.S. surveillance law to protect the rights of individuals in the European Union, including reforms to Section 702 of the FISA Amendments Act.[7] Two other nominations - Edward Felten and Jane Nitze - followed in March 2018.[8] While Adam Klein participated in a short confirmation hearing in February 2018,[9] not one of these three candidates have been confirmed, meaning the Board still has only one official member. Additionally, even if all three nominees were confirmed that would, with existing member Elisebeth B. Collins,[10] bring the PCLOB up to three members, including a chair, from the majority party, and a single member of the minority party, failing to provide for the balance of viewpoints achieved by the previous PCLOB and required by EU law as a criterion for an oversight body.[11]

- *The promulgation of an Executive Order that demonstrates a disregard for the rights of non-Americans*

Executive Order 13768 was signed by President Trump in his first full week in office.[12] The Order included a provision that served as an early indicator of the Administration's willingness to disregard even the most basic protections for non-Americans, including the right to privacy. Despite several legal challenges based on different sections of the Order, it remains in full effect.

- *The appointment to lead U.S. intelligence agencies of several individuals who have a record of undermining human rights*

In our letter to Commissioner Jourová from February 2017 calling into question the continued viability of the Privacy Shield, we flagged the appointment of CIA Director Mike Pompeo, U.S. Attorney General Jeff Sessions, and Director of National Intelligence Dan Coats as holding well-established views antithetical to the protection of the rights of Europeans within the United States. Since then, Mr. Pompeo has since switched roles to become the U.S. Secretary of State.[13]

---

[7] https://www.cnas.org/publications/congressional-testimony/adam-klein-before-the-senate-committee-on-the-judiciary; *see also* https://epic.org/2017/08/trump-nominee-to-head-privacy-.html.

[8] https://www.congress.gov/nomination/115th-congress/1751; https://www.congress.gov/nomination/115th-congress/1752.

[9] https://www.c-span.org/video/?440791-1/judiciary.

[10] https://www.pclob.gov/board-members/.

[11] Notably, the three majority party members are all licensed attorneys while Edward Felten, while incredibly accomplished, does not come from a legal background.

[12] https://www.dhs.gov/publication/executive-order-13768.

[13] https://www.newyorker.com/news/news-desk/with-mike-pompeo-at-the-state-department-are-the-uber-hawks-winning.

While there have been many shake-ups among U.S. Cabinet officials, current and former members, including the three we initially referenced, have continued to evince antipathy to human rights. This includes new CIA Director Gina Haspel, an abettor of torture programmes while she was an officer while she was an officer,[14] as well as White House Chief of Staff John Kelly, who not only defended torture, but also has been a vocal supporter of harsh policies for immigrants and refugees.[15] Additionally, Trump-appointed ambassador to the United Nations, Nikki Haley, shepherded the U.S. withdrawal from the UN's Human Rights Council, diminishing the body's ability to protect at-risk communities.[16] This unprecedented decision leaves doubt as to what, if any, commitment the United States maintains toward international human rights. The statements and actions of these officials appointed under the current U.S. Administration continue to demonstrate the abdication of its role as a global leader on human rights.

- *The status-quo allowing the application of expansions to Executive Order 12333*

The Trump Administration has taken no steps to further limit the expansions to EO 12333 enacted by the Obama Administration near the end of their tenure.[17] EO 12333 continues to authorise essentially any surveillance that takes places outside the U.S. and is targeted at non-U.S. persons, thus putting EU individuals at direct risk. Under Executive Order 12333, the U.S. conducts broad, inadequately overseen, non-transparent surveillance of innocent people and whole communities around the world without having to meet any evidentiary standard and without providing for redress mechanisms. These kinds of programmes collect users' address books and lists, and record details about every phone conversation and other forms of communications, across full countries. While the U.S. Administration considers these activities to be "targeted", they would qualify as indiscriminate and disproportionate surveillance in the EU based on the criteria developed by the Court of the Justice of the European Union in the *Schrems* case.[18] It is important to read the Commission implementing decision Recital 71 in this context when it refers to "a general rule of prioritisation of targeted over bulk collection" by the U.S. Intelligence Community and adds that "[a]ccording to the assurance provided by the ODNI, they ensure in particular that bulk collection is neither 'mass' nor 'indiscriminate', and that the exception does not swallow the rule".[19] Recital 72 adds about Presidential Policy Directive 28 (PPD-28) that while "Intelligence Community elements must sometimes collect bulk signals

---

[14] https://www.washingtonpost.com/outlook/i-went-to-prison-for-disclosing-the-cias-torture-gina-haspel-helped-cover-it-up/2018/03/15/9507884e-27f8-11e8-874b-d517e912f125_story.html?utm_term=.d191aa47c1e0.

[15] https://www.aclu.org/other/john-kelly-facts.

[16] https://www.accessnow.org/access-now-condemns-u-s-withdrawal-from-u-n-human-rights-council/.

[17] https://www.eff.org/deeplinks/2017/01/obama-expands-surveillance-powers-his-way-out.

[18] http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dd5e9098d5f1554057b0eba20524efa244.e34KaxiLc3qMb40Rch0SaxyOahr0?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=265961.

[19] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG&toc=OJ%3AL%3A2016%3A207%3AFULL#ntc69-L_2016207EN.01000101-E0069.

intelligence in certain circumstances, for instance in order to identify and assess new or emerging threats, it directs these elements to prioritise alternatives that would allow the conduct of targeted signals intelligence". The footnote of this addition, however, refers to a report to the U.S. President by the intelligence community "assessing the feasibility of creating software that would allow the Intelligence Community more easily to conduct targeted information acquisition rather than bulk collection. According to public information, the result of this report was that 'there is no software-based alternative which will provide a complete substitute for bulk collection in the detection of some national security threats".[20] Unlike what the Commission implementing decision concludes, we highlight that there is no guarantee that "bulk collection will only occur where targeted collection via the use of discriminants — i.e. an identifier associated with a specific target (such as the target's e-mail address or phone number) — is not possible 'due to technical or operational considerations'." As a consequence, the explanation and assurance provided by the ODNI might be in line with the loose interpretation of the U.S. Administration for "targeted" and "bulk" but it does not align with the EU Court of Justice's criteria.

- *The intelligence community's abandoned promise to provide necessary transparency into surveillance programs*

The debate over the reach of Section 702 of the FISA Amendments Act (FAA) ended in early 2018 when a bill was enacted that not only failed to meaningfully reform the authority but, in fact, extended its reach in many important ways. We will provide more information on this expansion below.

- *The failure to protect the rights of people in the EU in agreements used to bypass Mutual Legal Assistance Treaties (MLATs)*

Like the debates over Section 702 of the FAA, the debates over statutory changes to allow bilateral agreements to bypass the MLAT process also concluded this year with the passage of the Clarifying Lawful Overseas Use of Data (CLOUD) Act. The provisions of the CLOUD Act failed to ensure the protection of human rights, including rights of Europeans, within the agreements foreseen by the law. We provide additional information below.

### *1. Recent Developments in the U.S. Legal Framework*

You have asked for more information on relevant developments in U.S. legislative, regulatory, administrative, or case-law frameworks relevant to the effective operation of the Privacy Shield.

#### A. Legislative Changes

[20] http://icontherecord.tumblr.com/ppd-28/2015/overview.

In October 2017, mere months after the European Commission completed its first annual review of the Privacy Shield, Access Now provided a summary of important measures, both positive and negative, pending U.S. Congressional action.[21] Unfortunately, while the U.S. Congress moved to advance several pieces of legislation that we identified, the only proposals we have seen enacted are those that, rather than creating new safeguards for human rights, undermine their application. Below we provide more information on these provisions.

*a. FISA Amendments Reauthorization Act of 2017*

In September 2017, as the debate was still raging over what form (if any) the reauthorisation to the FISA Amendments Act would take, an editorial was penned by Robert Litt, the former General Counsel of the Office of the Director of National Intelligence (ODNI) and author of the letters regarding U.S. surveillance submitted along with the Privacy Shield.[22] In it he discusses at length the position of Tim Edgar, another former ODNI employee, that the U.S. surveillance regime should provide greater protections for the privacy of non-U.S. persons. Litt ultimately concludes, "[p]roviding extensive legal rights to foreigners outside the United States is...not justified."[23]

This is undoubtedly the position of the members of the U.S. Congress who voted to pass the FISA Amendments Reauthorization Act, which became U.S. law on January 19, 2018 after a temporary, stop-gap reauthorisation was passed at the end of 2017.[24] The final measure that was adopted was a conglomeration of the worst proposals considered by the U.S. Congress to reauthorise the otherwise-expiring FISA Amendments Act, including the now-infamous Section 702.[25] Unfortunately, what was packaged as a "reform bill" not only failed to implement any reforms that addressed the rights of Europeans, but in many ways it expanded the law's already over-broad provisions.

For example, lawmakers lauded the bill as placing a limitation on what is known as "about collection" (called "abouts collection" in the law).[26] As background, there were two primary

---

[21] https://www.accessnow.org/fall-cheat-sheet-u-s-congress/.
[22] https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q1F; https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q1A.
[23] https://www.lawfareblog.com/transparency-public-service-and-foreign-intelligence-thoughts-beyond-snowden.
[24] https://www.congress.gov/bill/115th-congress/senate-bill/139/text/eah; https://www.accessnow.org/happened-surveillance-bill-congress-week.
[25] https://www.accessnow.org/cms/assets/uploads/2017/12/Analysis-of-702-reform-bills-infographic.png.
[26] https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=826 (Temporarily ceases "abouts" collection—involving the collection of communications that refer to, but are neither to nor from, a specific target—until the Intelligence Community presents Congress with new procedures for "abouts" collection that address compliance concerns.). *See also* https://www.democraticleader.gov/newsroom/11118-2/ (And then on the [about] language... When it is used, they have to go to the FISA court and get permission, come to Congress for ratification of that. There are many protections there.).

surveillance programmes known to operate pursuant to Section 702: Prism, where the government would send directives to internet companies that required production of records, including the content of communications, to or from identified "selectors", and Upstream, in which the directives are sent to the services providers who operate the infrastructure of the internet who in turn briefly acquired and scanned all communications made over the wire for those same selectors.

About collection occurred when, during the scans conducted under Upstream, information would be captured not only to or from the selectors, but also communications that only referenced the selectors.[27] This practice was controversial and many saw it as unlawful.[28] In 2017, the U.S. National Security Agency announced it would be halting about collection, reportedly due to the inability to conduct the collection in line with limitations established by the Foreign Intelligence Surveillance Court (FISC), which is responsible for generally approving the surveillance.[29]

So, prior to the reauthorisation of Section 702, about collection was no longer occurring and presumed unlawful. In the reauthorisation, rather than codifying this cessation, which would have been a positive step, the U.S. Congress instead provided a clear and explicit path for the NSA to re-instigate the practice, requiring only a 30-day notice to the U.S. Congress before it begins anew.[30] It's hard to see how this provision is anything other than an *expansion* of NSA's ability to conduct surveillance, and certainly is not a limitation on what the agency can do.

This is just one of several examples of the way the 702 reauthorisation has been incorrectly framed as a reform or a check on U.S. surveillance operations. Other changes to 702 made in the reauthorisation had no impact on the reach of the law, particularly vis a vis non-U.S. persons, including individuals in the EU.

That is to say, not only have the pointed observations of the Court of Justice of the European Union in the Safe Harbor ruling not been remedied, but after many years the current state is actually less protective for Europeans than it was when we started. And to get here, the expansion of Section 702 was approved with conscious disregard of the existence of Privacy

---

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

[28] https://www.justsecurity.org/40384/ado-about/ ("about" collection seems hard to square with the Foreign Intelligence Surveillance Court's own understanding of the purported "foreign intelligence exception" to the Fourth Amendment's warrant requirement. According to partially declassified FISC opinions, a particularised warrant based on probable cause is not needed to intercept communications—even the communications of an American citizen—sent to or from an agent of a foreign power. But, of course, even if §702 "targets" are in practice limited to foreign agents—a restriction not found in the text of the statute—there is no reason to think a message that is merely about a target satisfies the exception, rendering it mysterious why interception would be constitutionally permissible absent a particularised probable cause warrant.).

[29] https://www.accessnow.org/privacy-victory-u-s-nsa-stop-collecting-communications-foreign-intel-targets/; https://www.nytimes.com/2017/04/28/us/politics/nsa-surveillance-terrorism-privacy.html.

[30] https://www.justsecurity.org/50801/house-intelligence-committees-section-702-bill-wolf-sheeps-clothing/.

Shield or the potential economic impact on the U.S. and the EU of failing to enact meaningful reforms.

In addition to the increased grant of authority, it is also noteworthy that the National Security Agency's Inspector General released an unclassified version of its Semi-Annual Report to Congress in July 2018, covering the period between October 2017 - March 2018.[31] Among other things, the report noted several incidents of non-compliance with rules on handling and transfer of surveillance information to foreign entities.[32] While reportedly non-intentional, these incidents highlight the need for greater transparency and stricter rules on the commission of surveillance and use of information derived therefrom.

*b. Clarifying Lawful Overseas Use of Data (CLOUD) Act*

The Clarifying Lawful Overseas Use of Data (CLOUD Act) became U.S. law in March 2018. The new law enables U.S. law enforcement to unilaterally obtain data stored abroad, under U.S. law, even absent an international agreement.[33] The CLOUD Act also allows the U.S. and countries to enter bilateral agreements to access data held by companies in one another's jurisdictions.[34]

Both ways in which the law expanded on law enforcement access to data in the control of companies abroad will likely increase the collection of European's data. This increased collection of EU persons data did not exist at the time of the adequacy determination conducted by the EU Commission and should be weighed against the safeguards and limitation of the Privacy Shield and the EU data protection acquis.

Article 48 of the GDPR, which addresses the transfer of EU data pursuant to an order of a non-EU country, limits transfers to those "based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. . . ."[35] CLOUD Act agreements may not satisfy the "international agreement" required by Article 48. While an MLAT requires the consent of the U.S. Senate, the U.S. Congress would have a more narrow veto authority to overturn a CLOUD Act agreement.[36] The text of the bilateral (or multilateral) agreement between the U.S. and a third country themselves will also govern process for data transfers, which may be unsatisfactory or inconsistent with EU law. Beyond Article 48 of the GDPR, it is for instance unclear how these agreements will interact with norms set under the EU Police Directive and the EU-U.S. Umbrella Agreement.
In that context, the Privacy Shield expands the amount of European data held in the U.S. and which can therefore be subject to requests by governments around the world through these

[31] https://www.oversight.gov/node/16349.
[32] https://www.oversight.gov/sites/default/files/oig-sa-reports/OIG%20UNCLASS%20SAR%20OCT-MAR%202018.pdf.
[33] 18 USC § 2713.
[34] 18 USC § 2523.
[35] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679.
[36] 18 USC § 2523(d).

agreements, including potential partners like the UK, whose surveillance laws have been challenged under EU law.[37]

Unilateral demands by U.S. law enforcement — like the demand issued by the U.S. for data stored in Ireland under the Microsoft-Ireland case — would pose the most direct challenge to compliance with the GDPR.[38] In the meantime, there is uncertainty as to whether the CLOUD Act permits the U.S. to reach an agreement with the EU or requires separate agreements with individual member states.[39] If an agreement cannot be made with the EU, there will likely be Member States which the U.S. would not reach an agreement and whose data would be subject to unilateral requests by the U.S. or other countries. These legislative developments driven by the U.S. might lead to fragmentation of laws and law enforcement practices among EU member states that would undermine the efforts to strengthen the trust and harmonisation in the field of justice, freedom and security of the European Union.

*c. Lack of action from the U.S. Congress*

The ways that the U.S. Congress has not acted may weigh as heavily on the continued viability of the Privacy Shield as the laws that they have passed. Several vitally important provisions have been introduced but not approved, leaving large gaps in U.S. law through which data of individuals in the EU can be manipulated and exploited.

Some of the measures that have not been enacted by the U.S. Congress include:

- **Data Protection** - Despite the increasing amount of attention paid to data protection in the United States as well as globally, the U.S. still does not have a comprehensive data protection law. In fact, the state of California, as of 2018, is the only state known to have passed such a provision. This lack of movement on data protection prevents the United States from being able to keep up on ensuring respect and protection for personal information.
- **Data Breach Notification** - While, as of 2018, all 50 U.S. states (and most territories) have a law on data breach notification, there is no federal standard, and the patchwork provides a lower level of protection than is required by the GDPR. Further, those standards that have been proposed on a federal level are much less protective than even many state laws and they all include a provision to pre-empt the stronger protections.
- **Modernizing the Electronic Communications Privacy Act (ECPA)** - Passed in 1986, ECPA no longer reflects the realities of the way users interact online and instead allows for much lower standards for law enforcement to access user data held for longer than

[37] https://www.wired.co.uk/article/uk-surveillance-unlawful-watson-davis
[38] http://www.scotusblog.com/case-files/cases/united-states-v-microsoft-corp/.
[39] https://www.lawfareblog.com/possible-eu-us-agreement-law-enforcement-access-data.

180 days. ECPA applies to both U.S. persons as well as non-U.S. persons.[40] As the Commission has indicated in its request for input, the U.S. Department of Justice recently changed its official policies on the issuance of non-disclosure orders (so-call "gag orders"), primarily in response to a lawsuit brought by Microsoft challenging the orders' constitutionality.[41] However, this policy does not extend to state or local agencies beyond the Department of Justice, does not answer the basic inadequacies of ECPA, and, without codification in law, could be reversed by either this or any future administration.

- **The PATCH Act** - When the U.S. government discovers or is notified about a previously unknown software vulnerability, they are meant to follow the Vulnerabilities Equities Process (VEP) to decide whether to disclose it for patching or hold it for offensive purposes. However, the process as it stands contains large loopholes and operates at the pleasure of the administration. The PATCH Act would create a review board to codify the VEP, establish a public disclosure policy, and periodically report on disclosures. This is necessary for ensuring that any data stored in the U.S. is protected against known or knowable exploits.[42]
- **The ENCRYPT Act** - Members of Congress, Officials at the Federal Bureau of Investigation (FBI), and other prominent government officials have issued ever-increasing calls to undermine encryption over the past several years. The ENCRYPT Act would not limit their interference, but prevent state legislatures from creating a patchwork of anti-encryption provisions.[43]
- **Cyber Shield Act** - As internet of things (IoT) devices continue to become more prevalent, it is important to ensure adequate protection of the data that they collect. The Cyber Shield Act creates an advisory committee to set cybersecurity standards for the internet of things for which compliance would give a certification. This would allow users to make more informed decisions about with whom to allow their data to be stored.

## B. Regulatory Changes

### *a. Treatment of non-U.S. persons and border surveillance*

On 25 January 2017, President Trump issued an Executive Order on "Enhancing Public Safety in the Interior of the United States" which strictly limits protections under the U.S. Privacy Act of 1974 to U.S. persons except as provided for by law.[44] This decision indicates a disregard for any ability for non-U.S. persons to access or correct data held on them by government agencies.

---

[40] https://privacylaw.proskauer.com/2011/10/articles/electronic-communications/ninth-circuit-ecpa-protects-stored-communications-of-foreign-citizens/.

[41] https://www.justsecurity.org/46875/modernizing-ecpa-congressional-action-dojs-gag-order-guidelines/.

[42] https://www.wired.com/story/vulnerability-equity-process-charter-transparency-concerns/.

[43] https://www.eff.org/deeplinks/2018/06/encrypt-act-protects-encryption-us-state-prying.

[44] https://www.whitehouse.gov/presidential-actions/executive-order-enhancing-public-safety-interior-united-states/.

This statement calls into question the continuation of protections provided by order of the U.S. Attorney General under the Judicial Redress Act.[45] Obtaining judicial redress for EU data subjects was one of the key demands from the European Union in order to conclude negotiations on the Umbrella Agreement and the Privacy Shield. The Judicial Redress Act grants a very limited right to remedy to non-U.S. persons in cases when their personal information has been misused under certain sections of the U.S. Privacy Act of 1974. This does not, however, protect people from misuse of data collected by federal agencies or in federal programs that have been made exempt from these protections. Nor would it allow them to initiate legal claims against companies for privacy breaches that take place in the U.S.

On 27 January 2017, President Trump issued another Executive Order, commonly known as the Muslim ban, restricting travel of visitors from certain Muslim-majority countries.[46] This EO included a provision calling for every immigrant to be screened to determine whether they would be "a positively contributing member of society," would "make contributions to the national interest," and whether they intended to commit a crime or terrorist act. As part of the application of the EO, the office of Immigration and Customs Enforcement (ICE), started developing an "Extreme Vetting Initiative" to conduct these assessments via automated decision making, including machine learning. Despite widespread opposition to this and other proposals, the U.S. State Department forged ahead to implement several "extreme vetting" practices for certain visa applicants "determined to warrant additional scrutiny" 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."[47]

In May 2018, ICE officials abandoned the idea to use machine-learning technology as part of the initiative and decided to instead rely on a contractor which will be tasked with analysing all the information received.[48] This decision does not negate the risks and harms associated with the social media monitoring put in place by the Extreme Vetting Initiative, now called "Visa Lifecycle Vetting". The programme continues to require certain visa applicants to provide social media identifiers, telephone numbers, and email addresses used in the past five years, among other information, thus facilitating the mining of information while privacy and data protection safeguards are unclear.

---

[45] https://www.congress.gov/bill/114th-congress/house-bill/1428.

[46] https://www.whitehouse.gov/presidential-actions/executive-order-protecting-nation-foreign-terrorist-entry-united-states/.

[47] https://www.federalregister.gov/documents/2017/08/03/2017-16343/60-day-notice-of-proposed-information-collection-supplemental-questions-for-visa-applicants.

[48] https://www.washingtonpost.com/news/the-switch/wp/2018/05/17/ice-just-abandoned-its-dream-of-extreme-vetting-software-that-could-predict-whether-a-foreign-visitor-would-become-a-terrorist/?noredirect=on&utm_term=.d39889754358.

These developments show a growing disregard for human rights by the U.S. Administration which put at risk the continued existence of PPD-28, which took the unprecedented but limited step of recognising privacy "interests" of all people. PPD-28 was central to the Privacy Shield negotiations but because it has never been written into law, it could be vacated unilaterally by the current administration.

The decreasing commitment of the U.S. government and its officials towards protecting individuals' right to privacy at the border can also be noted in the statement of Ambassador Nathan A. Sales, Coordinator for Counterterrorism at the U.S. State Department from July 2018.[49] Ambassador Sales indicated that the United States is not prepared to renegotiate its Passenger Name Record (PNR) agreement to prevent the EU from imposing additional restrictions in the processing of PNR data to increase travellers' privacy. The Court of Justice of the EU indeed declared a similar draft agreement with Canada to be incompatible with the EU Charter of Fundamental Rights, in particular with Articles 7 and 8 protecting the rights to privacy and data protection.[50] As Guardian of the Treaties, the EU Commission has the obligation to ensure the application of the jurisprudence from the Court and it cannot be dictated by U.S. officials on whether and how to reform an agreement if there are doubts with its compliance with the EU Charter.

### C. Common Law Changes

#### *a. Carpenter v. United States*

In June 2017, the Supreme Court of the United States (SCOTUS) agreed to hear the case *Carpenter v. United States*.[51] 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.[52] SCOTUS had previously held that a person did not have a privacy interest in information that was voluntarily shared with a third-party, such as a telephone provider. This jurisprudence known as the "third party doctrine" greatly differs from the EU approach under which users retain the privacy protections of the EU Charter of Fundamental Rights and EU secondary law even when data is shared with a third party, regardless of whether voluntary.

In June 2018, SCOTUS held that law enforcement must obtain a warrant under the Fourth Amendment of the U.S. Constitution to access an extended period of users' historical cell phone location data held by telecommunications companies.[53] The decision will bring the U.S.

---

[49] https://translations.state.gov/2018/07/19/counterterrorism-data-privacy-and-the-transatlantic-alliance/.

[50] curia.europa.eu/juris/document/document.jsf?text=&docid=183140&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=282786.

[51] http://www.scotusblog.com/case-files/cases/carpenter-v-united-states-2/.

[52] https://epic.org/amicus/location/carpenter/.

[53] https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf.

government's interpretation of privacy closer to its human rights obligation and establishes an opportunity to further challenge over-broad U.S. surveillance practices. The location data at issue in *Carpenter* provided the U.S.authorities "near perfect surveillance." Law enforcement had access to nearly 13,000 location points generated by a user's phone over 127 days, ubiquitous tracking enabled by the "seismic shift" in digital technology. Human rights law requires that government agents meet certain standards prior to surveillance, including surveillance of so-called public information when it hits the point where it reveals private data.[54]

Importantly the Supreme Court recognised that users have an expectation of privacy in widely collected location and movement data, which is highly sensitive and for which users have no real ability to opt-out. The *Carpenter* ruling expand users' privacy protections at a critical time as U.S. political leaders continue to disregard and even undermine global human rights. The decision shows a limit to long-established jurisprudence of the "third party doctrine." The doctrine however was not yet fully struck down and, as a result, the differences between the EU and the U.S. in the way to protect the right to privacy largely remains.

### *2. Compliance Monitoring and Enforcement*

#### A. The Federal Trade Commission

The U.S. Federal Trade Commission (FTC) is an independent body tasked with a mission to "protect consumers by preventing anticompetitive, deceptive, and unfair business practices, enhancing informed consumer choice and public understanding of the competitive process, and accomplishing this without unduly burdening legitimate business activity".[55] Traditionally, the FTC acts as an enforcement body rather than a supervisory authority with oversight powers in contrast with European data protection authorities. In the words of Chairman Joseph Simons, under the EU-U.S. Privacy Shield, the FTC is tasked with enforcing the "promises" voluntarily made by companies signing up to the Privacy Shield under its jurisdiction.[56] In a statement from July 2018 before a committee of the U.S. House of Representatives, Chairman Simons indicated that "the FTC has actively enforced Privacy Shield, and will continue to do so when Privacy Shield participants fail to meet their legal obligations" though no evidence of this enforcement was provided.[57]

Following massive data breaches such as Equifax and revelations about invasive data practices in the Facebook/Cambridge Analytica scandal, the FTC is facing increasing pressure to take action and address these privacy violations. Despite the agency's history of robust enforcement

---

[54] https://necessaryandproportionate.org/principles.
[55] https://www.ftc.gov/about-ftc.
[56] https://www.ftc.gov/system/files/documents/public_statements/1394526/p180101_ftc_testimony_re_oversight_house_07182018.pdf.
[57] https://www.ftc.gov/system/files/documents/public_statements/1394526/p180101_ftc_testimony_re_oversight_house_07182018.pdf.

in the competition area and landmark cases against online companies in the early 1990s at a time where only 5% of the U.S. population was online, the FTC has brought relatively few cases - though significant in size - against technology companies.[58] This can partly be explained by the way the FTC functions and is organised.[59] The FTC Bureau of Consumer Protection leads the agency privacy efforts and its lawyers are entrusted with case selection. The selected cases are then evaluated by economists from the FTC Bureau of Economics, who are often skeptical of initiating long privacy battles. In June 2018, Chairman Simons have announced that FTC officials will initiate a listening tour in 17 U.S. cities to get feedback from individuals, academics and others on how to tackle digital challenges, including online privacy.[60] This tour and the ongoing investigation of the FTC into Facebook following the Cambridge Analytica story will provide a clear indication of the FTC's ability and willingness to adequately enforce the right to privacy of U.S.-persons, as we continue to search for evidence of its enforcement of privacy rights of individuals in Europe.

### B. The Ombudsperson

The Privacy Shield created a new redress mechanism in the Privacy Shield Ombudsperson tasked with the specific mission to address issues of inappropriate state access to user data. 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.[61]

In our submission to the first annual review of the Privacy Shield, we wrote that the Ombudsperson mechanism is inadequate to provide protection that is essentially equivalent to that prescribed by EU law.[62] The Ombudsperson mechanism indeed does not meet the criteria for independence and lacks investigatory powers. What is more, since January 2017, the position was left vacant. For 19 months now, the U.S. Administration has blatantly disregarded what has repeatedly been identified by the EU as main priority for the functioning of the Privacy Shield.

In July 2018, Commissioner Jourová has written to Wilbur Ross, U.S. Commerce Secretary, to reiterate her call for an Ombudsperson and gave a deadline of three-months for the U.S. to

---

[58] https://www.cambridge.org/core/books/federal-trade-commission-privacy-law-and-policy/7699DD78299FAD8CA401005ACDEF0125.

[59] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2901526.

[60] https://www.washingtonpost.com/news/the-switch/wp/2018/06/20/how-should-the-feds-regulate-tech-this-government-watchdog-is-hitting-the-road-for-ideas/?noredirect=on&utm_term=.e9a15a27a23e.

[61] 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.).

[62] https://www.accessnow.org/cms/assets/uploads/2017/07/AN-PSReviewResponse-1.pdf.

comply with this demand.[63] We welcome this announcement by the Commission and expect expeditious action if comes October 2018 the Ombudsperson position would remain vacant (or is filled by a temporarily acting public official, as is currently the case). In the meantime, the structural flaws of the mechanism identified above shall be addressed through the annual review process.

### C. European Parliament and Data Protection Authorities

In November 2017, the Article 29 Working Party (WP29) - now replaced by the European Data Protection Board (EDPB) - published its findings for the first joint annual review of the Privacy Shield and made a series of concrete recommendations and demands to remedy systemic flaws of the arrangement and to address serious shortcomings in its implementation.[64] In particular, the WP29 indicated that by 25 May 2018, an independent Ombudsperson should be appointed as well as all PCLOB members. As of 31 July 2018, neither of these conditions have been fulfilled.

In its findings, the WP29 added that "in case no remedy is brought to the concerns of the WP29 in the given time frames, the members of WP29 will take appropriate action, including bringing the Privacy Shield Adequacy decision to national courts for them to make a reference to the CJEU for a preliminary ruling." This commitment was reiterated in January 2018 by the outgoing Chair of the WP29 during a public hearing in the LIBE Committee of the European Parliament.[65] Access Now calls on the members of the EDPB to refer the Privacy Shield to national courts as the identified shortcomings remain unaddressed.

In the meantime, the European Parliament have adopted in July 2018 a resolution calling for the suspension of the Privacy Shield arrangement unless the U.S. complies with EU data protection requirements by 1 September 2018.[66] The EU Parliament indicates in the adopted text that the current Privacy Shield arrangement does not provide the adequate level of protection required by Union data protection law and the EU Charter as interpreted by the CJEU and expresses concerns, among others, over the passage of the CLOUD Act, the continuous application of EO 12333 and, the reauthorisation of Section 702.

While the requests of the EU Parliament and the WP29/EDPB might not be legally binding, the Privacy Shield is under ongoing legal scrutiny, not only in a pending case before the General Court of the CJEU, but also by data protection authorities.[67] The EU Commission risks harming

---

[63] https://www.ft.com/content/f5c4795e-91b0-11e8-b639-7680cedcc421.
[64] https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782.
[65] http://web.ep.streamovations.be/index.php/event/stream/180129-1500-committee-libe.
[66] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2018-0315+0+DOC+XML+V0//EN&language=EN.
[67] http://curia.europa.eu/juris/fiche.jsf;jsessionid=9ea7d0f130da311665d9f91148d0a1b6f6bbf84e9381.e34KaxiLc3eQc40LaxqMbN4Pb3qTe0?id=T%3B738%3B16%3BRD%3B1%3BP%3B1%3BT2016%2F0738%2

both the economical interest to uninterrupted data flows and EU fundamental rights by not addressing existing flaws and deficiencies of the Privacy Shield. Access Now urges the Commission to take the recommendations of the WP29/EDPB and the EU Parliament into utmost consideration through this second annual review process.

### *3. Functioning of Redress and Review Mechanisms*

#### A. Cambridge Analytica/Facebook

In March 2018, *The New York Times* and *The Guardian* published stories about the relationship between a data analytics company called Cambridge Analytica and Facebook.[68] Both companies self-certified under the Privacy Shield framework.[69]

The story begins in 2014 when a group of social scientists led by Aleksandr Kogan created and deployed a personality test called "thisisyourdigitallife" via a Facebook app. This app allowed researchers to access personal information not only about app users but also their Facebook friends. These friends had not used the app and therefore could not have consented to the use of their data. This feature allowed Kogan and his team — along with potentially any other researcher with similar access — to harvest the information of a vast network of Facebook users. In this case, reports indicate that 50 million people could have had their data mined by Kogan.

In the background, Global Science Research (GSR), Kogan's company, had contracted to disclose the data he collected to Cambridge Analytica, which had invested in advertising for the app to increase the number of users who authorised its use. Cambridge Analytica analysed and used the data to create and purchase highly targeted ads that were used for the 2016 U.S. presidential elections, as well as potentially for other high-profile elections and debates such as the Brexit Referendum.

In 2015, after but not necessarily related to this incident, Facebook changed its rules to prohibit app developers from accessing the personal information of friends of app users.[70] Around the same time, Facebook asked Cambridge Analytica to delete the information that had been obtained through the personality test app which was originally intended to be used as data for social science research.[71] The company purportedly certified to have deleted the information. It is unclear whether Facebook took any meaningful steps to verify this was actually the case.

---

FP&pro=&lgrec=en&nat=or&oqp=&dates=&lg=&language=en&jur=C%2CT%2CF&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&num=T-738%252F16&td=%3BALL&pcs=Oor&avg=&mat=or&jge=&for=&cid=388686.

[68] https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

[69] https://www.privacyshield.gov/participant?id=a2zt00000008PdqAAE&status=Inactive; https://www.privacyshield.gov/participant?id=a2zt0000000GnywAAC&status=Active.

[70] https://techcrunch.com/2015/04/28/facebook-api-shut-down/.

[71] https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

In March 2018, Facebook suspended the accounts of Cambridge Analytica and its parent company, Strategic Communication Laboratories (SCL), due to whistleblower reports that the information was never deleted and was left insecure.[72]

Since then Facebook CEO and employees have testified in front of U.S. Congress, the UK Parliament and, the EU Parliament. Despite these testimonies, many questions and uncertainties remain as regards Facebook data practices. Access Now has called upon Facebook to undergo an independent audit of its data processing accompanied by a global human rights assessment, to complement any public investigation.[73] To date the company still has not responded to our open letter and request.

In the meantime, the UK Information Commissioner's Office (ICO) launched an overarching investigation into the use of data analytics in political campaigns.[74] As part of that investigation the ICO found that Facebook had violated the law by lack of transparency and security issues relating to the harvesting of data constituting multiple breaches of the data protection principles under the Data Protection Act 1998. Facebook now faces a £500,000 fine, the highest possible amount under the UK Data Protection Act prior the applicability of the GDPR.[75] The ICO is also investigating political parties and campaigns, Cambridge Analytica and other firms that may have been involved in the unlawful data processing practices.

In the U.S., the FTC has opened a non-public investigation into Facebook privacy practices.[76] In this context, the agency recalled its power to bring "enforcement action against companies that fail to honor their privacy promises, including to comply with Privacy Shield". The results of this investigation are yet to be known, as well as the extent to which compliance with the Privacy Shield Principles will be analysed.

Finally, we are unaware of any FTC investigation into Cambridge Analytica despite its self-certification under Privacy Shield.

### B. Redress mechanisms under Privacy Shield and redress for national security

[72] https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/.

[73] https://www.accessnow.org/cms/assets/uploads/2018/06/Open-letter-to-Facebook-from-Access-Now.pdf.

[74] https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf.

[75] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/07/findings-recommendations-and-actions-from-ico-investigation-into-data-analytics-in-political-campaigns/.

[76] https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection.

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."[77] 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, 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 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." Past experience shows FTC's enforcement activities have historically been limited to procedural requirements rather than investigating privacy and data protection practices of companies.[78]
- Binding arbitration by the "Privacy Shield Panel." This final redress mechanism is characterised 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.[79]

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.[80] This process is lengthy, opaque, and prevents people in the EU from exercising their rights within the United States.[81]

The Commission implementing decision also refers to avenues available under U.S. law to EU data subjects when their information is being processed by the U.S. Intelligence Community.

---

[77] 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.

[78] 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.).

[79] 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.

[80] Recital 56, *Id*.

[81] https://free-group.eu/2016/04/06/eu-us-privacy-shield-towards-a-new-schrems-2-0-case/.

This includes the possibility to bring a civil cause of action for money damages against the United States when information about them has been unlawfully and wilfully used or disclosed, to sue U.S. government officials in their personal capacity for damages or to challenge the legality of surveillance. In practice, the pursuit of these mechanisms can be complex, costly and, confusing in an unfamiliar jurisdiction. Additionally, access to courts can be further restricted on procedural grounds. It is common for claims brought by individuals - including U.S. persons - to be declared inadmissible due to a lack of "standing" whereby a plaintiff has to demonstrate to the court sufficient connection to and harm from the law challenged to support that participation in the case. Demonstrating standing can be particularly difficult given the lack of transparency of the U.S. Intelligence Community in the operations it conducts and the absence of a notice requirement to individual when their information have been processed. Finally, most of these limited remedies are also not available under certain programmes such as the EO 12333 which is particularly relevant for the surveillance of non-U.S. persons, including Europeans.

These difficulties are odds with the requirements set by the EU Court of Justice in the *Schrems* ruling regarding the right to an effective remedy before a tribunal.[82] Aware of these shortcomings, the EU Commission decided to create the Ombudsperson Mechanism as a way to help strengthen EU data subjects right to remedy. Access Now has strong reservations as regards the ability of such an Ombudsperson to effectively provide for a right to remedy given the flaws of the proposed mechanism identified in point 2.B of this submission.

In any case, the functioning and robustness of this mechanism could not be adequately tested so far as the position of the Ombudsperson has remained vacant for the last 19 months. As a result, the current implementation of the Privacy Shield does not meet the necessary EU Commission's requirement to guarantee EU data subjects' right to an effective remedy. Finally, beyond our comments about the inadequacy of the ombudsperson as a legal avenue and even with a permanent appointee, the possible lack of cases brought under the Ombudsperson mechanism cannot be considered as an evidence of the functioning of the Privacy Shield. Individuals are largely unaware of the way their information is processed and of the avenues available to seek redress in case of misuse of their data. While the Commission should do more to promote these mechanisms, we need to acknowledge the inherent lack of incentive to do so as such cases could put in jeopardy the existence of the adequacy decision approved by the Commission itself. NGOs and data protection authorities are the entities best placed to bring cases, however both of those have limited resources to initiate lengthy cases and, regrettably, no public funding is available for this activity.

### *4. Automated Decision Making*

82

http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dd5e9098d5f1554057b0eba20524efa244.e34KaxiLc3qMb40Rch0SaxyOahr0?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=265961.

The General Data Protection Regulation (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.[83] 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. Worse still, the Privacy Shield does not provide for safeguards regarding the use of automated decisions which produce legal effects or otherwise affect the individual.

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 processing, including profiling, takes place in the United States largely without limitation. U.S. law on automated decision making generally provides individuals with the possibility to opt-out of further sharing of their profile or to access 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.

Sectoral provisions in the area of credit rating exists in the U.S. where for instance the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act (FACTA) were developed to safeguard users against credit rating abuses, for instance by allowing user to contest mistakes in their credit ratings.[84] These frameworks 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.[85]

Through the first annual review of the Privacy Shield, companies asserted that none of the data transferred under the Privacy Shield are processed through automated decision making systems. However, WP29 concluded that the feedback provided by companies was not sufficient to determine "whether these assertions correspond to the reality of all companies adhering to the Privacy Shield".[86]

The difference in 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.

---

[83] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

[84] 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.

[85] https://epic.org/privacy/fcra/.

[86] https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782.

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. Since May 25, 2018, the GDPR, including updated data protection rights for users and new rules on the transfer of personal data, has becomes applicable and is now the legal basis of all adequacy decisions currently in place between the EU and other countries, including the Privacy Shield. In this context, we call on the Commission to analyse whether the Privacy Shield is equipped to protect the rights of persons in the EU, as guaranteed under the EU Charter and the newly applicable GDPR. In our view, the entry into application of the GDPR requires, at minimum, significant changes to the Privacy Shield, in the area of automated decision making and beyond.[87]

***Conclusion***

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

- Take the recommendations of the WP29 and the EU Parliament into utmost consideration;
- Amend the Privacy Shield to include effective individual redress mechanisms and independent oversight - beyond the appointment of an Ombudsperson - and invest in better promoting those mechanisms and raising awareness for people in the EU in how to pursue them;
- Amend the Privacy Shield to ensure compliance with the GDPR. 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.
- Ensure the meaningful participation of the European Data Protection Board, as well as the European Parliament and civil society, in this second review process; and
- Commit publicly to transparency by publishing all relevant documents, working papers, and findings from the review process.

We believe that these recommendations form the bare minimum requirements for the Privacy Shield to be brought up as close as possible to compliance with EU primary and secondary law. Nevertheless, the (expanded) U.S. surveillance framework and the recent detrimental attitude of the U.S. Administration towards the protection of human rights globally continue to undermine the validity of the arrangement. As negotiations with U.S. counterparts did not lead to significant progress in the functioning of the arrangement over the past 19 months, it is high time for the

[87] https://www.accessnow.org/cms/assets/uploads/2017/07/AN-PSReviewResponse-1.pdf.

Commission to take action for the protection of EU data subjects rights and suspend the arrangement.

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