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

26 July 2019

Re: Access Now Responds to Privacy Shield Review Questionnaire - Third review

Dear Mr. Gencarelli,

Thank you for your invitation to provide information and observations on the European Commission's third annual review of the EU-U.S. Privacy Shield arrangement, the mechanism to facilitate the transfer and processing of the personal data of individuals from the European Union to and 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 a presence in 13 locations around the world, including in the policy centers of Washington, DC and Brussels.[2] Access Now regularly analyzes data transfer arrangements under EU law, including the Safe Harbor arrangement that was invalidated by the Court of Justice of the European Union in 2015, and the Privacy Shield which replaced it.[3] Users benefit from a free, open, and secure internet that is enabled by legal certainty for stakeholders to operate. Robust data transfer frameworks which ensure a high level of data protection in the free flow of data are key to deliver these benefits for all actors.

The Privacy Shield continues to be inadequate to protect fundamental rights.
Since negotiations began in 2016, Access Now has provided detailed analysis and recommendations to the EU Commission on how to improve the Privacy Shield. To protect users' privacy and data protection when personal data is transferred, we have called on the EU and the U.S. to conduct comprehensive and necessary reforms.[4] These include surveillance reforms on both sides of the Atlantic and the enactment of a binding data protection framework in the U.S. and access to remedy for non-U.S. persons, including data subjects in the EU. In the absence of these important reforms, **the Privacy Shield has manifestly failed to meet the standards set by EU law** from inception to today.

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. Through the yearly

[1] Access Now
[2] Access Now - About Us
[3] Access Now - Privacy Shield
[4] Access Now - Blog - Activating the EU-US Privacy Shield: To protect privacy, we need reform, not rebranding

review processes, we have identified a series of privacy violations and shortcomings that disproportionately interfere with people's rights.

The Privacy Shield weakens Europe's data protection and privacy framework, and its global leadership role.
With the adoption of the General Data Protection Regulation, the EU has become a global leader in the protection of personal data around the world. The EU has begun exercising positive influence in other regions, helping to drive political conversations that should contribute to raising the global state of data protection for users around the world.

However, the EU's reputation, leadership role and its influence are severely hindered by allowing incompliant arrangements like the Privacy Shield that manifestly fail to meet the standard of EU law and compromise rights and values. With the world watching, the EU cannot afford to contradict itself and let the United States continue to undermine human rights without consequence.

The Privacy Shield arrangement should be suspended now.
Since its adoption in 2016, the situation with the Privacy Shield has only deteriorated. Over the past two years, there has been a notorious expansion of surveillance powers in the U.S. while the U.S. Administration has shown disdain at the country's long term commitment to human rights, including privacy rights of U.S. and non-U.S. persons. Under these circumstances, and for the reasons further detailed in our submission, **we call on the EU Commission to suspend the Privacy Shield arrangement to protect EU data subjects' rights**.

To assist the EU in this process, we answer the European Commission's request for comments. For this third review, you have specifically asked us to provide feedback on the following areas:

- Relevant developments in U.S. law (legislative, regulatory, administrative or case-law developments) since October 2018;
- The prospect of the adoption of a federal privacy law and how it could improve the protection of privacy in the U.S.;
- Mechanisms for compliance, enforcement, and oversight, including activities conducted by the Federal Trade Commission (FTC).

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 for the third annual review." We do not have additional comments to provide the EU Commission this year regarding the area of automated decision-making, but we refer to comments submitted in the two previous review processes which remain applicable.[5]

[5] Access Now - Submission to First Privacy Shield Review and Access Now - Submission to Second Privacy Shield Review

To assess the functioning of the Privacy Shield and the commitment of the U.S. administrations, we will start by providing a summary of relevant developments in EU and U.S. laws and practices since 2016. We will then address each of the topics put before us by the EU Commission in turn.

I. Summary of relevant developments in EU and U.S. law and policies from February 2016 to July 2018

A. Developments in U.S. law identified by Access Now in responses to previous reviews and communications with the EU Commission

February 2017 letter to EU Commissioner Věra Jourová

In February 2017, Access Now wrote to Commissioner Jourová and LIBE Chair Claude Moraes.[6] We highlighted several developments in the U.S. that we thought significantly impacted the United States' commitments under the Privacy Shield, including:

- 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; and
- 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."[7]

Access Now Response to the Privacy Shield First Annual Review Questionnaire

In our response to the first review of the Privacy Shield conducted in 2017, we explained to the EU Commission that the U.S. had taken actions related to its surveillance programs that undermine transparency and demonstrate a broadly held opinion in the U.S. Congress and Administration "that non-U.S. persons, including people in the EU, do not and should not have cognizable human rights protections."[8] We further reported on the evidence provided by the Foreign Intelligence Surveillance Court (FISC) showing willful misuse of surveillance authorities by the U.S., including Section 702. As we then explained, the debate over the use of Section 702 is relevant to the Privacy Shield. Despite some reforms and years of debates, mass surveillance is still lawfully permitted under a few authorities in the U.S., including Section 702 and Executive Order 12333. The operation of programmes under Section 702 were central to the invalidation of the Privacy Shield predecessor, the Safe Harbour, by the Court of Justice of the European Union (CJEU).[9]

---

[6] Access Now - Letter to EU Commissioner Jourova on the impact of new U.S. policies and regulatory frameworks on the privacy rights of users in Europe
[7] *Id*.
[8] Access Now - Submission to First Privacy Shield Review
[9] Court of Justice of the European Union - Case C-362/14 - Schrems

In the second annual review process, Access Now noted that the situation of the already flawed Privacy Shield has deteriorated. Through 2017 and 2018, "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."[10] In particular, we highlighted the negative impact on the validity of the Privacy Shield due to:

- The promulgation of Executive Order 13768 that demonstrates a disregard for the rights of non-Americans, including the right to privacy;
- The appointment to lead U.S. intelligence agencies of several individuals who have a record of undermining human rights;
- The status-quo allowing the application of expansions to Executive Order 12333;
- The intelligence community's abandoned promise to provide necessary transparency into surveillance programs; and
- The passage of FISA Amendments Reauthorization Act of 2017, which not only failed to implement any reforms that addressed the rights of Europeans, but in many ways expanded the law's already over-broad provisions.

B. Developments in EU. law identified by Access Now in responses to previous reviews and communications with the EU Commission

Entry into application of the EU General Data Protection Regulation

On May 25, 2018, the General Data Protection Regulation (GDPR) became applicable. The processing of personal data in the EU is based on the GDPR which provides for different mechanisms to transfer personal data to third countries, including adequacy decisions. As we mentioned in our response to the first review of the Privacy Shield, the application of the GDPR means that all decisions, including the Privacy Shield, should be reviewed in line of the updated and strengthened data protection rules. The upcoming first review on the implementation of the GDPR is an opportunity for the EU Commission to reform all adequacy decisions, including the arrangement with the U.S., and to bring them fully in line with the requirements of the GDPR.

In 2017, we called on the EU Commission to:

1. **Ensure the application of the principle of purpose limitation as defined under the GDPR**

   The principle of purpose limitation is included in the Privacy Shield without specific definition.[11] The lack of definition means there are no criteria limiting the scope of collection and use of personal information as is provided in the GDPR.[12]

[10] Access Now - Submission to Second Privacy Shield Review
[11] Point 5 of the Privacy Shield Principles.
[12] Article 5.1.b of of Privacy Shield, Article 6.4 of the GDPR.

2. **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 disclosure of user data to third parties and for expansion in the uses of the data beyond why it was initially collected.[13] The concept of opt-out is intrinsically different to "consent" as defined under the GDPR: opt-out requires no affirmative action and creates an additional burden for the data subjects.

3. **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.[14] The Privacy Shield does not indicate what mechanism is available to exercise this right, either in the context of "regular" processing of data or through 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 processing, including profiling, can (and does) take place in the United States largely without limitation.[15]

   While we call for the suspension of the Privacy Shield arrangement, these recommendations remain valid today for the negotiation of potential future adequacy decision with the U.S.

Recommendations of EU Data Protection Authorities and Resolutions of the EU Parliament

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.[16]

In July 2018, the European Parliament adopted a resolution calling for the suspension of the Privacy Shield arrangement unless the U.S. complies with EU data protection requirements.[17] 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.

[13] Privacy Shield Principles Point 2a on Choice; Article 4.11 of the GDPR.
[14] Article 22 of the GDPR.
[15] EPIC - Credit Scoring
[16] Article 29 Data Protection Working Party - EU – U.S. Privacy Shield – First annual Joint Review
[17] European Parliament resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield

In our response to the second review of the Privacy Shield, we mentioned that 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.[18] The EU Commission risks harming both the economical interest to uninterrupted data flows and EU fundamental rights by not addressing existing flaws and deficiencies of the Privacy Shield.[19]

II. Relevant developments in U.S. law since October 2018

The United States has made some progress over the past year to comply with its obligations and commitments under the Privacy Shield. For instance, after unacceptable delays, the Privacy Shield ombudsperson was at last confirmed by the U.S. Senate. However, this mechanism is inadequate to provide protection that is essentially equivalent to that prescribed by EU laws (see relevant section below).[20] Additionally, the Privacy and Civil Liberties Oversight Board has a fully-confirmed membership for the first time since 2016 and has announced important new projects, though with limited impact for non-U.S. persons.[21] In fact, while programs operated under Executive Order (EO) 12333 are on the agenda, it says little about the extent those reviews will focus on non-U.S. persons. This is significant since EO 12333 provides authority for a large amount of surveillance activities directed against people outside the United States, including people living in the European Union whose rights are protected under the EU Charter.

Despite these developments, there are several places where U.S. law, policy, and operations continue to invade the rights of data subjects in the European Union, many of which we analyze in more detail below.

A. Agreements under the U.S. CLOUD Act

In 2018, the United States and the United Kingdom began negotiations to enter into an agreement to allow law enforcement in each jurisdiction to have direct access to information stored in the other country. As we explained in our submission in 2018, the U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act allowed the Department of Justice to enter these agreements, but did not require adequate protections for human rights. Neither the U.S. nor UK governments have indicated a willingness to require the protections that would be necessary to protect the data of people in the EU from broad government access to their data in violation of the European Convention on Human Rights, the EU Charter, and international law.[22] Once reached, an

[18] Court of Justice of the European Union - Case T-738/16 - La Quadrature du Net and Others v Commission
[19] Access Now - Submission to Second Privacy Shield Review
[20] Covington - Privacy Shield Ombudsperson Confirmed by the Senate
[21] PCLOB - Privacy and Civil Liberties Oversight Board Welcomes Senate Confirmation of New Members; see also PCLOB - The Privacy and Civil Liberties Oversight Board has voted to initiate three new oversight projects, including a review of the use of facial recognition and other biometric technologies in aviation security
[22] Access Now - Blog - Protecting our privacy under the CLOUD: what new agreements should look like

agreement would exacerbate the worst aspects of both country's surveillance laws, not to mention any other government with which the U.S. pursues a similar arrangement.[23]

The EU is also exploring the possibility of more agreements under the U.S. Cloud Act while still assessing the validity of the processing. In July 2019, the EU Data Protection Board (EDPB) sent a letter to the EU Parliament providing a legal assessment of the impact of the U.S. Cloud Act on the European legal framework for personal data protection. In this thorough analysis, the EDPB concludes that, at the time of publication and, in the absence of a warrant recognised or made enforceable on the basis of an international agreement, the lawfulness of transfers of personal data under requests made by U.S. law enforcement authorities through the U.S. CLOUD Act for criminal investigation purposes "cannot be ascertained."[24] Instead, the EDPB calls for an improvement and update of the Mutual Legal Assistance Treaty (MLATs) already in force between the EU and the U.S. as it "contains only very limited provisions relevant from a data protection point of view." Access Now has also called on states to focus their efforts in reforming MLATs to guarantee the rule of law and safeguards for users. To that end, we have published detailed recommendations to improve these mechanisms in a way that protects privacy and advances the rights of users.[25]

B. Increased border surveillance and use of invasive technologies

U.S. Government documents continue to reveal the increasing scope of surveillance at the U.S. border. This surveillance is indicative of the U.S. government exercising greater authority to violate the privacy of people, particularly non-U.S. persons. In January 2019, documents from the U.S. Bureau of Customs and Border Protection (CBP) demonstrated how the Administration was creating dossiers with the personal information of people providing assistance to asylum-seekers, but also that they were being targeted for enhanced screening during U.S. border crossings.[26] Further, a lawsuit filed by the American Civil Liberties Union forced the disclosure of documents from CBP and the U.S. Immigration and Customs Enforcement (ICE) that showed both agencies "asserting near-unfettered authority to search and seize travelers' devices at the border, for purposes far afield from the enforcement of immigration and customs laws."[27] Unfortunately, even lawmakers who have opposed the more extreme "border security" measures proposed by the Trump Administration have supported the adoption of much greater surveillance, including drones, biometric scans and facial recognition, and "risk-based targeting" that seems to imply racial profiling.[28]

C. Misuse of surveillance authorities

The USA FREEDOM Act was passed to reform part of U.S. surveillance law known as "Section 215." In 2013 it was revealed, due to documents made available by Edward Snowden, that Section

[23] Access Now - Blog - If a U.S.-U.K. CLOUD Act agreement fails to protect our rights, the risks could go global
[24] EPDB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection
[25] Access Now - Blog - We need to fix the broken system for cross-border access to data
[26] CDT - Coalition Letter to DHS Opposing Surveillance of Activists, Journalists, and Lawyers
[27] ACLU - We Got U.S. Border Officials to Testify Under Oath. Here's What We Found Out
[28] Washington Post - More border surveillance tech could be worse for human rights than a wall

215 was being used to indiscriminately collect records of phone calls that either originated or terminated in the United States.[29] The USA FREEDOM Act was intended to prevent this sort of bulk collection from happening again. However, the collection taking place under the reform continues to increase, and the agencies have failed to comply with the transparency requirements.[30]

In June 2018, the U.S. National Security Agency (NSA) announced that, due to "technical irregularities" the Agency has collected information that it was not entitled to under the USA FREEDOM Act, and that the information could not be separated.[31] To remedy the error, the NSA decided to purge the entire database.[32] Later that year, the compliance incident was repeated, and the database had to be purged once again.[33] Potentially as a result of these incidents, the program was reported to have been shut down in early 2019.[34] However, adequate transparency has not yet been provided into the extent or the rationale for the decision.[35] Further, the remaining failures in transparency have meant we do not know if the program has really stopped or moved under another, broader authority under an interpretation that could allow the collection of more information with fewer limitations and safeguards. Despite all of this, officials in the White House have signaled that they may seek permanent reauthorization of the authority.[36]

III. Prospect of the adoption of a federal privacy law in the U.S.

A. U.S. Congress will likely not adopt a federal data protection law before the November 2020 U.S. presidential election

While civil society advocates, academics, and other policy stakeholders had hoped that the United States Congress was primed to pass a federal privacy law in the near future, it seems very unlikely that this will happen before the November 2020 U.S. presidential election. A bipartisan working group has been meeting over the past year to work out the details of what that law may look like, though so far the results of those meetings have not been made public. It is unclear how much progress has been made towards a comprehensive human-rights respecting law. However, several hearings have been held to discuss issues around privacy and data protection that will likely inform the final product in positive ways.

Unfortunately, there are voices that advocate for provisions that would deliver an unacceptably-weak law, which would have long term consequences for the protection of rights as well as the ability for U.S. legal structures to adapt to changing circumstances. For example, certain industry groups, such as the Information Technology Industry Council, have lobbied for broad carve outs for their businesses from a potential future law. Equally concerning, trade groups,

[29] The Guardian - NSA collecting phone records of millions of Verizon customers daily
[30] EFF - EFF and 23 Civil Liberties Organizations Demand Transparency on NSA Domestic Phone Record Surveillance
[31] The New York Times - N.S.A. Purges Hundreds of Millions of Call and Text Records
[32] *Id*.
[33] Washington Post - Repeated mistakes in phone record collection led NSA to shutter controversial program
[34] See *id*. See also The New York Times - Disputed N.S.A. Phone Program Is Shut Down, Aide Says
[35] Access Now - Privacy advocates call on U.S. Congress to release information crucial for surveillance reform debate
[36] The Washington Post - White House has signaled it may seek permanent renewal of controversial surveillance power

such as the American Association of Advertising Agencies, have pushed for the law to have high thresholds for application, such as only applying to companies that make a certain amount of profit from the sale of data (thus leaving out business models based on advertising, which represent a large part of the online economy) or that have a certain number of employees. These industry proposals are incompatible with an all-encompassing law that meaningfully protects the rights of the individual. If industry succeeds in crafting the final law in line with these provisions, it will be an insufficient law.

The debates over a potential data protection law have perhaps been most contentious over two issues: a private right of action and the existence and scope of federal preemption.

A private right of action concerns the ability for individuals to challenge, in their own name, the failure to comply with the law, and is an important element that must be included in any federal privacy proposal. This right is vital to meaningfully protect the rights of users at risk because "[m]arginalized communities historically have not been able to rely upon the government to protect their interests."[37] Without a private right of action, individuals would have to rely on other institutions and mechanisms to vindicate their rights. Unfortunately, as explained elsewhere in this submission, the Federal Trade Commission has not yet demonstrated that it has the resources to adequately enforce its current authority on the topic of privacy, let alone additional legal rights or obligations.

Separately, any proposal that provides for anything but exceptionally narrow federal preemption will have negative consequences in both the short and long term. Federal preemption describes when a federal law is used to negate state law and/or prevent states from legislating on the same field in the future. While some argue that preemption is an "all or nothing" proposition, there are actually many forms that preemption provisions could take. For example, "conflict preemption" would only impact state laws that are directly inconsistent with the federal requirements. By contrast, "field preemption" could be used to prevent states from passing or enforcing any law related to privacy. There are also several ways to draft a clause on federal preemption between these two extremes.

Unfortunately, any form of preemption that extends beyond the most narrow provisions to protect direct conflicts between state and federal laws could freeze privacy protections in the U.S. and prevent the overall framework from being effectively updated as new or different ways that data could be manipulated appear.

It is important that states do not have their hands tied when it comes to protecting human rights. State governments are able to move more quickly than the U.S. Congress and respond to new threats as they occur. State laws can also contribute to driving political conversations forward at the federal level. It must be noted that without the passage of the California Consumer Privacy Act in September 2018, conversations about a federal law would possibly not be happening.[38] Extensive preemption could void the California Consumer Privacy Act, and if broad enough, could also impact the Illinois Biometric Information Privacy Act, state data breach notification laws, data security laws,

[37] Civil Society Joint Letter - Letter to Congress on Civil Rights and Privacy
[38] California Legislative Information - The California Consumer Privacy Act of 2018

civil rights protections, and a range of other important protections that state legislators have spearheaded.[39]

As the current debates around a private right of action and federal preemption indicate, it is far from ensured that a U.S. privacy law will provide meaningful protections that are on par with those contained in the EU's General Data Protection Regulation. The discussions around a privacy law should not reassure EU regulators and decision-makers that the U.S. will live up to its responsibility to pass a comprehensive statute.

B. State level legislation

In light of the U.S. federal government's inaction, several states have developed their own privacy legislation.

As previously referenced, the state of California passed the California Consumer Privacy Act (CCPA) in September 2018. It will go into effect in January 2020. The CCPA is similar to the GDPR, but differs in substantial ways. For example, the CCPA does not explicitly focus on accountability measures like the GDPR. The GDPR also requires a legal basis to process personal data, while the CCPA does not.

In addition, in June 2019, the state of Maine passed the Act to Protect the Privacy of Online Consumer Information. It will go into effect in July 2020. The Act mandates that internet service providers receive permission from users in order to share information with a third party. It is touted as the nation's strictest data protection law because, unlike the CCPA, individuals do not have to request that their data not be sold; it should not be sold by default.

Many other states are currently considering data protection legislation. It is likely that states will continue to enact their own privacy laws in light of the federal government's continued inaction.

C. The National Institute of Standards and Technology process

The National Institute of Standards and Technology (an agency of the U.S. Department of Commerce) is currently developing a "Privacy Framework" in consultation with industry, academic, and civil society stakeholders. The Framework is a voluntary enterprise risk management tool. The final Framework is expected to be released in early 2020. While we believe the final product has potential to provide a roadmap for companies to consider how to think about and incorporate privacy protections, the means and extent to which it is used will be at the discretion of individual organizations. Further, while we are supporting its development beyond the need to comply with the privacy laws, either in the U.S., the EU, or elsewhere, many may still see it as a compliance tool used singularly to meet strict legal obligations. Given the lack of a U.S. federal data protection law, the Framework could encourage industry to better incorporate privacy protections where there are no requirements, but it will not ultimately replace the need for affirmative rights, standards, and obligations.

[39] Illinois General Assembly - Biometric Information Privacy Act

IV. Mechanisms for compliance, enforcement, and oversight

A. The Federal Trade Commissioner jurisdiction and authority

On June 6, 2018, the U.S. Court of Appeals for the Eleventh Circuit issued its opinion in *LabMD, Inc. v. Federal Trade Commision*.[40] The case challenged the FTC's ability to take action against a company for poor data security practices and require implementation of a reasonable data security program.[41] The Court vacated the FTC's order under the notion that the sought remedy did not involve a specific act or practice and, therefore, was too vague. This decision has jeopardized the future of the FTC's jurisdiction to take action against companies with poor security practices. Absent a federal law, the FTC's authority in this action was the best placed to effectively curb the most negligent practices, though it remains in question if and to what extent the FTC can act, as well as what remedies are available.[42]

Additionally, despite endless revelations about invasive and unacceptable practices at Facebook, the FTC, with which Facebook has been under a decree order to, among other things, implement a comprehensive privacy program,[43] has only just issued a record-breaking fine against the company.[44] The announced $5 billion USD fine has been met with skepticism following reports that Facebook has merely written the fine into its quarterly statements as a one-time loss to be offset by earnings.[45] In fact, the day the decision was leaked to the press, Facebook's stock prices went up significantly which demonstrate that the fine remains too low to change the company behaviour and meaningfully reform its privacy invasive practices.[46] Both the drastically delayed action as well as the insufficient proposed remedy in the settlement raise questions about the FTC's ability to meaningfully protect privacy in the United States.

B. The Ombudsperson and other avenues for redress under the Privacy Shield

After two and a half years of promises coming from the U.S. administrations and clear demands from the EU institutions, the Privacy Shield ombudsperson has been confirmed by the U.S. Senate.[47]

As explained in previous review processes, the Privacy Shield created a new redress mechanism in the Ombudsperson tasked with the specific mission to address issues of inappropriate state access to user data in the U.S. The Privacy Shield specifically explains that the arrangement would

[40] United States Court of Appeals for the Eleventh Circuit - LabMD vs Federal Trade Commission
[41] Wiley Rein - FTC Rebuked in LabMD Case: What's Next for Data Security?
[42] IAPP - Takeaways from the 11th Circuit FTC vs. LabMD decision
[43] Federal Trade Commission - Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises
[44] Federal Trade Commission - FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook
[45] Politico US - Facebook expects up to $5B FTC fine
[46] The Verge - Facebook's $5 billion FTC fine is an embarrassing joke
[47] Covington - Privacy Shield Ombudsperson Confirmed by the Senate

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.[48]

While we welcome the fact that the U.S. is at least living up to its commitment under the Privacy Shield to complete the nomination process of the Ombudsperson, the mechanism remains inadequate to provide protection to the right to remedy that is essentially equivalent to that prescribed by EU law.[49] The Ombudsperson mechanism does not meet the criteria for independence. 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."[50] Furthermore, 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.[51]

In addition, the Ombudsperson mechanism lacks investigatory powers. The Privacy Shield claims that "the Ombudsperson mechanism provides for independent oversight with investigatory powers." [52] However, the Ombudsperson's role is limited and does not entail investigatory powers.[53] 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 and does not grant any authority for the Ombudsperson to investigate practices within agencies. In short, the Ombudsperson has no legal powers to enforce the rights of people in the EU against the U.S. government.

Similarly as with the Ombudsperson, other avenues for redress available or mentioned under the Privacy Shield do not allow people to meaningfully exercise their rights and reach an enforceable decision unless they go through almost all avenues to reach the Privacy Shield Panel.[54] This process is lengthy, opaque and prevents people in the EU from exercising their rights within the United States.[55] This means that the 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 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.

V. Other information relating to the implementation of the Privacy Shield

[48] EU Commission - Privacy Shield Adequacy Decision: "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.".
[49] Access Now - Submission to First Privacy Shield Review
[50] Access Now - Blog - Three facts about US surveillance the European Commission gets wrong in Privacy Shield
[51] Court of Justice of the European Union, C-288/12, C-518/07, C-614/10, C-362/14
[52] EUR-Lex - Recital 124 of the Privacy Shield
[53] Recital 124 of the Privacy Shield, *Id*.
[54] Recital 56, *Id*.
[55] FREE Group - "EU-US Privacy Shield: Towards a New Schrems 2.0 Case?"

A. Legal developments in the European Union

Pending cases in front of the Court of Justice of the European Union

This summer, the CJEU held a hearing in the case C-311/18 related to a complaint filed with Ireland's data protection authority by privacy activist Max Schrems. Schrems claimed Facebook violated the EU's data protection standards by allowing U.S. authorities to have unlawful access to data.[5657]

Schrems' complaint was linked to the mass surveillance revelations by Edward Snowden. After lengthy legal proceedings in Ireland, the case was sent to the EU Court in Luxembourg to determine the validity of the mechanism for transfer, a Standard Contractual Clause (SCC) used by Facebook, and clarify the powers of the DPA. However, the case could have implications for data transfers beyond SCCs as the Court also asked a series of questions about the legality of the separate Privacy Shield arrangement. The validity of the adequacy decision granted by the EU Commission under the Privacy Shield is also being challenged in the Tribunal in Luxembourg by a group of French NGOs and providers of internet access. The Tribunal has decided to put the Privacy Shield case on hold until the Court has resolved the SCCs case. This means that the Court may use the SCCs case to decide on the validity of the Privacy Shield. At the heart of the two cases are the surveillance practices in the U.S. One of the main questions is whether U.S. practices on processing of personal data by public authorities and agencies can co-exist with requirements under European data protection law.

While we await for the resolution of these cases, we reiterate our call to the EU Commission to suspend the Privacy Shield arrangement. As we have detailed in our analysis and submissions since 2016, the U.S. has not adequately reformed surveillance programs used towards non-U.S. persons, including data subjects in the European Union. What is worse, over the past three years, the protection of human rights, including the right to privacy, has deteriorated in the U.S. and a number of surveillance programs have expanded.[58] This means that most of the privacy and data protection violations that the Court had identified in the Safe Harbor case that led to its invalidation remain in place today. Until the U.S. implements appropriate reforms to remedy these privacy violations, they will remain a threat to the digital economy.

EU Parliament resolution on Cambridge Analytica

In October 2018, the European Parliament adopted a resolution on the use of Facebook users' data by Cambridge Analytica and the impact on data protection. In this text, the Parliament reiterated calls to suspend the Privacy Shield arrangement and called "on the U.S. authorities responsible for enforcing the Privacy Shield to act upon such revelations without delay."[59] Many of

[56] Court of Justice of the European Union - Case C-311/18 - Facebook Ireland and Schrems and NOYB - CJEU Case Schrems II
[57] NOYB Blog - CJEU hears case on EU-US data transfers (Standard Contractual Clauses and Privacy Shield)
[58] Access Now - Submission to Second Privacy Shield Review
[59] European Parliament resolution on the use of Facebook users' data by Cambridge Analytica and the impact on data protection

the entities involved in the Cambridge Analytica scandal, including Facebook and Cambridge Analytica itself, are self-certified organisations under the EU-U.S. Privacy Shield and, as such, benefited from the adequacy decision as a legal ground for the transfer and further processing of personal data from the European Union to the United States. In July 2019, following an investigation that took over a year to conclude, the U.S. Federal Trade Commission has voted to fine Facebook a record-setting $5 billion for privacy violations in relation to this scandal.[60] While it is important to see enforcement action coming from the FTC, the decision will have limited impact on the company and stronger actions are needed to change the invasive practices of the platform to protect users' rights.

Conclusion

Despite timid efforts by the U.S. to finally honor its commitment under the Privacy Shield after over two and a half years of inaction, the laws and practices of the U.S. continue to undermine the human rights of data subjects in the European Union. It is therefore high time for the EU Commission to suspend the arrangement.

We appreciate the difficult position of the European Commission as the viability of the Privacy Shield rests largely on the scope and implementation of U.S. law, which the Commission cannot control or change. Having said that, as Guardian of the Treaties, the Commission has the power and duty to ensure the enforcement of EU law, including the rights enshrined under the EU Charter. The EU Commission cannot allow the United States to continue to undermine the human rights of data subjects in the EU without consequence. The change of leadership in the EU institutions following the European elections is an opportunity to act on this matter.

Thank you again for the opportunity to provide feedback on this process. If you have any additional questions or would like more information on any of the points we raise in this comment, you may contact our policy experts below. We look forward to the results of your review.

Sincerely,

Estelle Massé
Global Data Protection Lead

Jennifer Brody
Legislative Manager

[60] Federal Trade Commission - FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook