



February 28, 2017

Attn:

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

CC:

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

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

Andrus Ansip
Vice-President, Digital Single Market
European Commission

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

Dear Commissioner Jourová,

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

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

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

Rights Ireland judgments², people in the EU are afforded appropriate privacy protections and redress in cases where their data is transferred to the US.

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

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

² Case C-293/12, *Digital Rights Ireland v. Minister for Comm.*, 2006 EUR-Lex 24 (Apr. 8, 2014), <http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=403885>.

³ In addition to the concerns outlined in that letter, we note that surveillance conducted under Executive Order (EO) 12,333, also violates the standards articulated by the Court of Justice in *Schrems*. This surveillance, which the US government largely conducts outside US soil, implicates EU citizen communications as they are in transit from the EU to the US. *See* Eur. Comm’n, Implementing Decision, Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, ¶ 75 (Dec. 7, 2016) *available at* http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf. Notably, EO 12,333 is the primary authority under which the NSA conducts foreign intelligence, and it encompasses numerous bulk collection programs that involve acquiring communications on a generalized basis, without discriminants. *See, e.g.*, Letter from ACLU to Privacy and Civil Liberties Oversight Board (Jan. 13, 2016), <https://www.aclu.org/letter/aclu-comments-privacy-and-civil-liberties-oversight-board-its-review-executive-order-12333>. In PPD-28, the US effectively acknowledged and ratified its bulk collection practices under this authority. *See* Press Release, White House Office of the Press Secretary, Presidential Policy Directive—Signals Intelligence Activities: Presidential Policy Directive/PPD-28 (Jan. 17, 2014), <https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>.

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

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

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

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

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

In addition, they emphasized that any legislation:

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

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

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

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

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

⁷ *Schrems*, *supra* note 1 at ¶ 91.

⁸ *Id.* at ¶ 95.

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

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

¹¹ *Id.* at article 18

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

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

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

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

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

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

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

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

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

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

2. Privacy and Civil Liberties Oversight Board

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

Even with a fully-functioning PCLOB, we had serious concerns that there was not effective oversight of US surveillance activities, and we strongly disagreed with many of the US government’s assertions in this arena. However, notwithstanding these concerns, it is clear that the European Commission relied on the representations regarding the oversight role of the PCLOB as part of its adequacy determination. Unfortunately, however, the PCLOB is no longer a fully functional body. Currently four of the five board positions on the PCLOB are vacant.¹⁹ Without a quorum, the PCLOB cannot issue reports and recommendations, including its planned report on activities conducted under executive order 12333 and the implementation of PPD-28.²⁰ In addition, the Board is further limited in its ability to make staffing decisions necessary to fulfill its responsibilities.²¹ Moreover, the vacancies also impact the extent to which the Board’s membership represents diverse political viewpoints. Under statute, no more than three of the Board members may come from the same political party, ensuring that a full Board contains representation from both political parties. The current membership, however, represents only one political party.

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

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

¹⁷ Comm’n Implementing Decision, *supra* note 8 at ¶ 95.

¹⁸ *Id.* at Annex VI.

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

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

²¹ *Id.*

Sincerely,



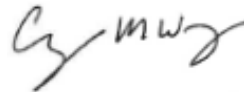
Faiz Shakir
Director
American Civil Liberties Union



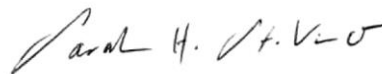
Lotte Leicht
European Union Director
Human Rights Watch



Neema Singh Guliani
Legislative Counsel
American Civil Liberties Union



Cynthia M. Wong
Senior Internet Researcher
Human Rights Watch



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