November 13, 2015

Secretary Penny Pritzker
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, D.C. 20230

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

Dear Secretary Pritzker and Commissioner Jourová,

We write to you on the occasion of your meeting this week concerning the future of EU-US data flows. We appreciate your interest in this important issue. Data protection is the foundation of trust for the Internet economy. It is for this reason that a "Safe Harbor 2.0" *per se* will not provide a viable framework for future transfers of personal information.

The Court of Justice of the European Union ("CJEU") has made clear that it is the "domestic law" and the "international commitments" of the United States that will determine whether future data transfers to the United States will be permitted.

For the reasons set out below, we urge you to commit to a comprehensive modernization of privacy and data protection laws on both sides of the Atlantic.

I. The *Schrems* Judgment

In most direct terms, the CJEU found that a trade arrangement between the US and the EU was invalid because it failed to ensure the protection of fundamental rights under the European Charter of Fundamental Rights ("Charter"). The Court also found that independent data protection agencies have the legal authority to enforce the rights set out in the Charter as against future decisions by the European Commission under Art. 25(6) of the Data Protection Directive of 1995. The Court's opinion creates a strong presumption that any similar framework -- a "Safe Harbor 2.0" -- will also be found invalid.

Background

Noting the original text of the Data Protection Directive of 1995, the CJEU restated the central point in the current debate over transborder data flows:

> [T]he object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognised both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, and in the general principles of Community law; ..., for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community; [1]

And describing the authorities of national data protection authorities to protect privacy, the CJEU noted further:[2]

> [T]he establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data; . . . such authorities must have the necessary means to perform their duties, including powers of investigation and intervention, particularly in cases of complaints from individuals, and powers to engage in legal proceedings; ...'

The central determination for transfers to Third party countries was set out in Article 25(1) of 95/46, which states:

> The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

The Court noted that in 2000, the European Commission made a determination that the adequate level of protection for the transfer of data from the Community to the United States "should be attained if organisations comply with the safe harbour privacy principles for the protection of personal data transferred from a Member State to the United States."[3] The Safe Harbor determination required that organizations should be "subject to the jurisdiction of the Federal Trade

---

[1] 95/46 Preamble 10 at Judgment, par. 3.
[2] 95/45 Preamble 62, 63 at Judgment, par. 3.
[3] Decision 2000/520 5 at Judgment par. 6. *See* 95/45 Art. 25(6).

Commission (FTC) . . ., or that of another statutory body that will *effectively* ensure compliance with the Principles implemented in accordance with the FAQs."[4]

The Authority of the National Data Protection Agencies

The CJEU spoke directly to the failure of the Irish Data Protection Commissioner to address the facts set out in the Schrems complaint. The Irish Commissioner concluded she had no authority to investigative alleged violations of the Directive in light of the Safe Harbor determination of the Commission. The CJEU rejected this conclusion.

The Court underscored the significant developments in caselaw since the adoption of the initial Safe Harbor, emphasizing the "importance of both the fundamental right to respect for private life, guaranteed by Article 7 of the Charter, and the fundamental right to the protection of personal data, guaranteed by Article 8."[5] The Court further emphasized the central responsibility of the independent national supervisory authorities as "an essential component of the protection of individuals with regard to the processing of personal data."[6]

As a consequence the Court determined that where a person "whose personal data has been *or could be* transferred to a third country," which is subject to Commission decision such as the original Safe Harbor or a proposed "Safe Harbor 2.0," asserts that the decision is incompatible with the protection of privacy and fundaments rights and freedoms, "it is incumbent upon the national supervisory authority to examine the claim with all due diligence. "[7] Moreover, even if the DPA rules against the complainant, the CJEU makes clear that "have access to judicial remedies enabling him to challenge such a decision adversely affecting him before the national courts. "[8]

The Invalidity of the Safe Harbor Arrangement

To understand the Court's conclusion that the Safe Harbor arrangement of 2000 was invalid, it is important to recognize that the Court placed great emphasis on the term "ensures" in Art. 25(1) of Directive 95/46. (The term appears 17 times in the judgment). That provision states:

> The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to

[4] *Id.* (emphasis added)
[5] Judgment par. 39.
[6] Judgment par. 41. *See* 95/46, Art. 28(3).
[7] Judgment par. 63 (emphasis added).
[8] Judgment par. 64.

compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question *ensures* an adequate level of protection. [9]

The other key term in the Court's analysis concerns the determination of "adequacy." The Court concludes that this does not require an "identical" level of protection to that guaranteed in the EU Legal system. However, relying on the opinion of the Advocate General, the CJEU concludes that a third party country "must ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is *essentially equivalent* to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter. "[10]

The next provision in the Court's opinion is key to understand why the United States must update domestic privacy law for transborder data flows to continue. The Court says directly "It is clear from the express wording of Article 25(6) of Directive 95/46 that it is *the legal order of the third country covered by the Commission decision that must ensure an adequate level of protection*."[11] Acknowledging that systems of law may vary, the Court concludes "those means must nevertheless prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union."

Noting both recent developments in EU law and the concerns about transfers of personal data "large number of persons whose fundamental rights are liable to be infringed," the Court "reduced" the authority of the Commission to make decisions under Art. 25(6) and states that subsequent determinations should be "strict."[12]

Regarding the derogations in the original Safe Harbor for "national security, public interest, or law enforcement requirements," the Court explains that "limitations in relation to the protection of personal data to apply only in so far as is strictly necessary."[13] The implications for current U.S practices here become clear. Article 7 of the Charter will require the end of the mass collection of the contents of electronic communications.[14] Article 47 of the Charter will require "*effective* judicial redress" which, the Court underscores, is "inherent in the existence of the rule of law."[15]

---

[9] Art. 25(1).
[10] Par. 73 (emphasis added).
[11] Par. 74 (emphasis added), par. 96.
[12] Par. 78.
[13] Par. 92.
[14] Par. 94.
[15] Par. 95 (emphasis added).

One other key phrase must be emphasized in the *Schrems* opinion: "domestic law or international commitments." This is the language that appears in Ar. 25(6) and is the basis for the Commission's legal authority to negotiate with the United States:

> The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its *domestic law or of the international commitments* it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.[16]

The phrase appears more than a dozen times in the Court's opinion. The intent is clear: the evaluation of adequacy of data transfers to the United States going forward will be based on the domestic law and international commitment of the United States.

II. The Proposed Framework

The Revised Framework, proposed by the European Commission, in November 2013, followed repeated calls to suspend Safe Harbor and the specific revelations that the National Security Agency had direct access to the personal information of Europeans transferred to Internet firms, operating in the United States.[17]

The 13 recommendations from the European Commission to update the Safe Harbor are:[18]

Transparency

1. Privacy policies should be publically posted on companies' websites in clear and conspicuous language. It is not sufficient for companies to provide the Department of Commerce with a description of their privacy policy.

2. Privacy policies of self-certified companies' websites should always include a link to the Department of Commerce Safe Harbor website, which lists all the

[16] 95/46, Art. 25(6).
[17] "Restoring Trust in EU-US data flows – Frequently Asked Questions," European Commission – Memo/13/1059. November 27, 2013. http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm. See http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf
[18] http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf

"current" members of the scheme. Since March 2013, the Department of Commerce has requested this from companies, but the process should be intensified.

3. Self-certified companies should publish privacy conditions of any contracts they conclude with subcontractors, e.g. cloud computing services. Safe Harbor allows onward transfers from Safe Harbor self-certified companies to third parties acting as "agents," for example to cloud service providers by contract that provides at least the protection of the Safe Harbor. When entering such a contract, a Safe Harbor company should also notify the Department of Commerce and make the privacy safeguards public.

4. Clearly flag on the website of the Department of Commerce all companies that are not current members of the scheme. However, in the case of "Not current," the company is obliged to continue to apply the Safe Harbor requirements for the data that has been received under Safe Harbor.

Redress

5. The privacy policies on companies' websites should include a link to the alternative dispute resolution (ADR) provider and/or EU panel. This will allow European data subjects to contact the ADR or EU panel in case of problems. Since March 2013, Department of Commerce has requested this from companies, but the process should be intensified.

6. ADR should be readily available and affordable. Some ADR bodies in the Safe Harbor scheme continue to charge fees from individuals – which can be quite costly for an individual user – for handling the complaint ($200-250). By contrast, in Europe, access to the Data Protection Panel to solve complaints under the Safe Harbor is free.

7. The Department of Commerce should monitor more systematically ADR providers regarding the transparency and accessibility of information they provide concerning the procedure they use and the follow-up they give to complaints.

Enforcement

8. Following the certification or recertification of companies under the Safe Harbor, a certain percentage of these companies should be subject to ex officio investigations of effective compliance of their privacy policies (going beyond control of compliance with formal requirements).

9. Whenever there has been a finding of non-compliance, following a complaint or an investigation, the company should be subject to follow-up specific investigation after one year.

10. In case of doubts about a company's compliance or pending complaints, the Department of Commerce should inform the competent EU data protection authority.

11. False claims of Safe Harbor adherence should continue to be investigated.

Access by US authorities

12. Privacy policies of self-certified companies should include information on the extent to which U.S. law allows public authorities to collect and process data transferred under the Safe Harbor.

13. It is important that the national security exception foreseen by the Safe Harbor Decision is used only to an extent that is strictly necessary or proportionate.

Viewed in light of the S*chrems* decision as well as the experience of consumer organizations on both sides of the Atlantic, it is clear that these principles will do little to reestablish trust for consumers. In brief:

- The provisions on "transparency" carry forward a "notice and choice" regime that fails to safeguard fundamental rights. The provisions fail to provide users with access to particularized information about the collection, use, and transfer of their personal information. The principles do not address the critical need to make public "the logic of the processing," i.e. "algorithmic transparency."[19]

- The provisions on "redress" rely on dispute resolution techniques that disfavor consumers and that fail to protect fundamental rights. It is clear that in disputes between consumers and businesses, ADR provides neither fairness nor justice. A recent series in the New York Times has made clear that ADR is no longer a viable means for consumers to seek legal recourse.[20]

---

[19] 95/46, Art. 12(a).

[20] Jessica Silver-Greenberg and Michael Corkery , "Arbitration Everywhere, Stacking the Deck of Justice," N.Y. Times, Oct. 31, 2015, available at http://www.nytimes.com/2015/11/01/business/dealbook/arbitration-everywhere-stacking-the-deck-of-justice.html; Jessica Silver-Greenberg and Michael Corkery, "In Arbitration, a 'Privatization of the Justice System'," N.Y. Times, Nov. 1, 2015, available at http://www.nytimes.com/2015/11/02/business/dealbook/in-arbitration-a-privatization-of-the-justice-system.html. The so-called Judicial Redress Act does not create a right of redress for violations of Safe Harbor.

- Finally, the provisions on "enforcement" carry little force after the *Schrems* decision. The reliance on Article 8 of the Charter in the Judgment makes clear that a framework for transborder data flows requires enforcement by an independent data protection agency. This baseline requirement is not even addressed in the revised framework. The United States does not have such an agency. It is therefore almost certain that the CJEU, or any of the data protection agencies within the EU will find a "Safe Harbor 2.0" invalid.

In short, there is nothing in the proposed revisions that improve "the domestic law" or "international commitments" of the United States as required by the *Schrems* judgment. The proposals merely revise a set of self-regulatory principles that lack legal effect.

III. Meaningful Reform of Data Protection

Consumer groups on both sides of the Atlantic are eager to see the governments of the European Union and the United States update privacy laws after the *Schrems* decision. We believe this is absolutely critical to ensure the continuation of transborder data flows. In broad terms we favor (1) the end of mass surveillance by intelligence agencies, (2) the establishment and modernization of legal frameworks that protect fundamental rights, (3) increased transparency and accountability for organizations that collect and use personal data, and (4) effective means of oversight and enforcement by independent data protection authorities.

As the negotiators set out 13 proposed changes to Safe Harbor prior to the *Schrems* decision, we have set out the 13 proposals for the EU and the US [6+6+1] that we believe are necessary after the judgment:

- The EU should enact an effective General Data Protection Regulation before the end of this year.

- The EU should enact a revised Directive on Data Protection in the context of Law Enforcement that provides greater accountability and transparency for police agencies and greater rights for individuals.

- The EU should end the mass surveillance of people by member states.

- The EU should suspend the Swift Agreement and the PNR Agreement and pursue a Digital Bill of Rights as recommended by the European Parliament Committee on Civil Liberties, Justice, and Home Affairs.[21]

[21] LIBE Committee, "Electronic Mass Surveillance of EU Citizens: Protecting Fundamental Rights in a Digital Age," (2013-2014). See also LIBE, "Mass surveillance: EU citizens' rights still in danger, MEPs say" (Oct. 13, 2015).

- The EU should enforce the data retention ruling of the CJEU in *Digital Rights Ireland* and prevent Member States from adopting laws that violate the fundamental rights to privacy and data protection.

- The EU should ensure effective enforcement of its data protection laws towards companies established in the US that are targeting users in Europe.

- The US should enact a comprehensive legal framework for data protection based on the Consumer Privacy Bill of Rights with appropriate regulatory and enforcement powers.

- The US should establish an independent data protection agency.

- The US should end the mass surveillance of non-US persons under Section 702 of the Patriot Act.

- The US should update the Privacy Act of 1974 to provide meaningful judicial redress to all person whose data is stored by a US federal agency.

- The US should ratify Council of Europe Convention 108, the Privacy Convention.

- The US should stand up for strong encryption and reject any law or policy that would undermine the security of consumers and Internet users.

- The EU and the US should commit to annual summit with the full participation of civil society organizations to assess progress toward these goals.

IV. Conclusion

A revised Safe Harbor framework similar to the earlier Safe Harbor framework will almost certainly be found invalid by the national data protection agencies and ultimately by the CJEU. In a recent Communication the Commission also acknowledges that it must ensure that "a new arrangement for transatlantic transfers of personal data fully complies with the standard set by the Court."[22] It is impossible to ignore that the *Schrems* decision requires necessary changes in the "domestic law" and "international commitments." Any proposal from the

---

[22] Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the Unites States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems), COM(2015) 566 final (Nov. 6, 2015).

Department of Commerce and the European Commission that attempts to substitute a trade pact for fundamental rights set out in Articles 7, 8, and 47 of the Charter will be subject to "strict" review by the CJEU.

We urge negotiators to confront the challenge that this moment presents. Failure will almost certainly lead to disruption of data flows and uncertainty for consumers and businesses on both sides of the Atlantic.

Sincerely,

EU Organizations

Belgian League of Human Rights
Bits of Freedom
Bulgarian Helsinki Committee
Centre for Peace Studies (Croatia)
Chaos Computer Club
Code Red
Digital Rights Ireland
Digitalcourage
European Association for the Defense of Human Rights
European Digital Rights
French League of Human Rights
Hungarian Civil Liberties Union
Initiative für Netzfreiheit
Italian Coalition for Civil Liberties
Liberty
Open Rights Group
Oživení (Czech Republic)
Panoptyon Foundation
Pištaljka
Privacy International
Public Concern at Work (UK)

US Organizations

Bill of Rights Defense Committee
Center for Digital Democracy
Consumer Action
Constitutional Alliance
Consumer Federation of America
Consumer Watchdog
Cyber Privacy Project
Defending Dissent Foundation
Electronic Privacy Information Center

Government Accountability Project
Patient Privacy Rights
Privacy Rights Clearinghouse
Privacy Times
Public Citizen
Restore the Fourth