Trans Atlantic Consumer Dialogue

Coordinated by Consumers International

DOC NO: INFOSOC 54/16 DATE ISSUED: 7 April 2016

Resolution on the EU-U.S. Privacy Shield Proposal

Introduction

On 29 February 2016, the European Commission and the Obama Administration released the proposed EU-U.S. Privacy Shield. The Privacy Shield aims to replace the Safe Harbour framework for commercial data flows between the EU and the U.S., which was struck down by the Court of Justice of the European Union in October 2015. The Privacy Shield agreement is to serve as the basis for an "adequacy" decision by the European Commission that the U.S. has a satisfactory system regarding data protection, including addressing issues related to government surveillance and consumer privacy.

The Transatlantic Consumer Dialogue (TACD) urges the European Commission not to adopt the Privacy Shield. This scheme does not adequately protect consumers' fundamental rights to privacy and data protection, as established in the EU Charter of Fundamental Rights and the 1995 Data Protection Directive, seen in the light of the European Court of Justice decision on Safe Harbour[1]. TACD believes that the Privacy Shield does not provide the necessary basis for a decision that the U.S. offers effective and meaningful data protection. The failure of the U.S. to have a robust overarching data protection law that ensures the privacy of its own citizens and consumers creates a barrier to any serious consideration on adequacy. We believe that the Privacy Shield will fail under the legal scrutiny of European Data Protection Authorities and, eventually, the European Court of Justice. What is required is a sustainable arrangement that guarantees privacy protection and legal certainty, based on needed changes in both the EU and US.

The TACD adopts the following recommendations to restore trust in digital economy and create a framework that guarantees the protection of EU and US consumers' personal information, allowing for data transfers over the Atlantic for the benefit of consumers and businesses alike.

TACD Recommendations

The TACD urges the **EU Authorities** to:

1. Hold off on adopting the proposed Privacy Shield decision, or any similar decision, until the United States can guarantee an essentially equivalent level of data protection to the one existing in the EU. This should include essentially equivalent rights for 'data subjects', as well as effective and independent oversight and redress mechanisms.

2. Publish a detailed legal review of the Privacy Shield *vis a vis* the European Court of Justice Safe Harbour ruling, the 1995 Data Protection Directive, the upcoming General Data Protection Regulation and the EU Charter of Fundamental Rights.

[1] Judgement of 6 October 2015, Case-362/14

3. Effectively enforce the EU data protection rules to stop unlawful data transfers to the United States. National Data Protection Authorities should fulfill their legal obligation to protect the fundamental rights of Europeans.

4. Formally adopt the agreed EU General Data Protection Regulation without delay, and urgently proceed with the review of the e-Privacy Directive, which should ensure full respect for the right to data protection enshrined in the Charter of Fundamental Rights, as interpreted and applied by the European Court of Justice, in the online environment.

5. Hold off on signing the EU-U.S. Umbrella Agreement, which is in itself a violation of fundamental rights. The Judicial Redress Act does not provide meaningful protections for data collected on non-U.S. persons (see Recommendation 5 below).

6. Instigate those Member States engaging in mass surveillance of individuals to put an end to such practices and respect the European Convention on Human Rights and the EU Charter of Fundamental Rights.

The TACD urges the **United States Authorities** to:

1. Enact a comprehensive legal framework for data protection and privacy. Without strong legal requirements governing the collection, use and retention of data for commercial purposes, we do not believe the Privacy Shield, or any similar arrangement can protect the privacy of either EU or U.S. consumers.

2. Become a full party, without undue reservations, to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) and its Additional Protocol regarding supervisory authorities and trans-border data flows (CETS No. 181), which are both open to non-European states and provide the widest internationally-agreed data protection standards.

3. Provide rulemaking authority to the Federal Trade Commission, so it can adopt safeguards on privacy and on data marketing and collection practices, and ensure that the Federal Communications Commission and the Consumer Financial Protection Bureau act on their respective jurisdictions and exercise the full extent of their rulemaking authority to protect consumer privacy in the electronic communications and financial services areas.

4. Establish an independent agency for the protection of privacy to ensure independent enforcement of the Privacy Act, develop additional recommendations for privacy protection and provide permanent leadership within the federal government on this important issue. The 'Ombudsperson' introduced by the Privacy Shield within the State Department is neither independent nor substitute for such an agency for consumer privacy and data protection. Additionally the 'Ombudsperson' competence is limited to government surveillance-related issues. The new independent agency should also have the appropriate enforcement and regulatory powers.

5. Update the Privacy Act of 1974 to provide meaningful judicial redress to any person whose data is

stored by a U.S. federal agency. The Judicial Redress Act does not provide meaningful protections for data collected on non-U.S. persons. The bill, as adopted, coerces European countries to transfer data to the U.S., even without adequate protection, or be denied legal rights[2].

6. Support strong encryption and reject any law or policy that would undermine the security of consumers and internet users. Strong encryption improves cybersecurity, promotes economic growth, and protects human rights.

7. End mass surveillance of U.S. and non-U.S. persons and enact a surveillance reform and legislative changes within a reasonable time.

The TACD urges the **EU and U.S. Authorities** to:

1. Commit to an annual transatlantic privacy summit[3] with the full participation of civil society organisations to assess progress toward the goal of achieving strong common data privacy standards on both sides of the Atlantic. The EU and the U.S. human rights and consumer protection groups play a key role to safeguard privacy and other civil liberties in order to balance the asymmetry of powers between governments, companies and individuals. The summit should serve as a basis for improving the level of data protection and the EU and the U.S. should give an official response to the recommendations made by civil society.

Background

The Safe Harbour Framework was an industry-oriented, self-regulatory approach to privacy protection that was repeatedly criticized as inadequate by the TACD. The TACD urged EU and U.S. decision makers on several occasions[4] to abandon the arrangement, which failed to provide adequate privacy protection for consumers in the United States and Europe.[5] The inadequacies of Safe Harbour are equally true for the proposed Privacy Shield Principles.[6]

On 6 October 2015, the European Court of Justice issued its ruling on Safe Harbour. In a historic victory for Europeans' privacy rights, the Court declared Safe Harbour invalid on the basis that it did not comply with the requirements set out in EU data protection law, read in light of the EU Charter of Fundamental Rights. The Court also declared that European data protection authorities have the power to examine with complete independence whether the transfer of a person's data to a third country complies with the requirements laid down by European law.

[2] https://epic.org/foia/umbrellaagreement/EPIC-Statement-to-HJC-on-HR1428.pdf and http://www.dailydot.com/politics/what-is-the-judicial-redress-act-europe-data-privacy-bill/
[3] In line with the proposal made by the Commission in its Communication: http://bit.ly/1XiYkxv
[4] http://test.tacd.org/wp-content/uploads/2013/09/TACD-ECOM-24-01-Implementation-of-the-Safe-Harbour-Agreement.pdf , http://test.tacd.org/wp-content/uploads/2013/09/TACD-ECOM-18-00-Safe-Harbour.pdf
[5] http://test.tacd.org/wp-content/uploads/2013/09/TACD-ECOM-08-99-Safe-Harbour-Proposal-and-International-Convention-on-Privacy-Protection.pdf
[6] Id. "It lacks an effective means of enforcement and redress for privacy violations. It places unreasonable burdens on consumers and unfairly requires European citizens to sacrifice their legal right to pursue privacy complaints through their national authorities. The Proposal also fails to ensure that individual consumers will be able to access personal information obtained by businesses."

At the center of the EU legal framework for the transfer of personal data from the EU to a third country, such as the U.S., is the notion of 'adequacy' in terms of the level of data protection provided in the third country in question. The Court interprets that 'adequacy' means that the third country must ensure, through its domestic legal order or international commitments, a level of protection which is essentially equivalent to that

guaranteed within the EU. U.S. legislation permitting mass surveillance and the lack of access to judicial redress in the U.S. for EU citizens, mean that the U.S. does not, in practice, pass the 'adequacy' test.

Consumers do not want the disruption of transatlantic data flows but their privacy must not be compromised by commercial interests and political pressure. The EU and U.S. privacy regimes contain fundamental differences in approach and substance. In the U.S. there is no statutory recognition of privacy as a fundamental right, unlike in the EU. In the EU there are strong data protection rules and principles that apply to any commercial collection and use of personal data, while in the U.S. this remains largely unregulated except in certain narrow sectors. For example, the unrestrained and massive data mining and consumer profiling practices of the commercial companies that can result in real harms, such as identity theft and discrimination, are not addressed effectively by legislation in the U.S.

The European Commission and the U.S. Department of Commerce announced that they reached a political agreement on transatlantic data flows on 2 February 2016. The negotiators, however, did not make the agreement public until 29 February.

In our judgement, the Privacy Shield proposal, however, does not provide significantly stronger protections than Safe Harbour. In the continuous absence of a U.S. legal privacy framework that meets the standards set in the EU, the Privacy Shield is generally flawed for the same reasons as its predecessor, and fails to ensure the essentially equivalent level of protection required under EU law. It also fails to bring any improvement whatsoever to the privacy protection of U.S. consumers. Importantly, like its predecessor arrangement, it continues to be a self-declared, self-regulatory system, which will be adhered to by a limited number of companies.

Such a self-regulatory proposal cannot substitute a regulatory system and leaves the language about the future actions of the Department of Commerce and the Federal Trade Commission an empty promise. U.S. tech companies are free to continually gather large quantities of personal data without meaningful legal constraints. The new framework does not seem to be providing any extra resources for the U.S authorities to enforce this arrangement effectively and proactively.

In terms of enforcement, which was one of the main flaws of Safe Harbour, in the absence of jurisdiction, an effective enforceable mechanism, and appropriate investigative and fining powers in the U.S., the role of European Data Protection Authorities has not improved substantially.

There are further deficiencies and ambiguities in the Privacy Shield proposal, and it fails to address the requirements stemming from the European Court of Justice ruling, specifically:

- It is unclear from the proposed text whether and how Data Protection Authorities will be able to suspend data flows. This one flaw in itself prevents the Privacy Shield from bringing legal certainty for businesses and consumers.

- The proposed Choice principle only limits data processing to disclosure to a third party or when there is a material change of purpose. This protection does not only exclude other forms of data collection and use but also violates the principle of purpose limitation. If a company defined the purpose for data processing broad enough, it is easy to circumvent any restraints the Privacy Shield proposal would impose.

- There are disproportionate exemptions to apply opt-out rules for processing sensitive data instead of requiring companies to obtain affirmative express consent.

- The proposal also fails to provide meaningful judicial redress mechanisms. Alternative Dispute Resolution is not essentially equivalent to judicial redress for an individual.

- Taking into consideration the strong connection between the private companies massive data gathering and mass surveillance: U.S. surveillance practices characterized as targeted are still considered "bulk" under EU law.

- The Ombudsperson within the State Department tasked to resolve surveillance-related questions from individuals does not qualify as independent.

Therefore, the Privacy Shield does not and cannot change the existing fundamental imbalance between EU and U.S. privacy regimes, which will be further enhanced by the upcoming EU General Data Protection Regulation. The United States must make changes to its domestic laws and international commitments to improve its privacy framework and bring it up to EU standards. It is the only way to guarantee a high level of privacy protection for consumers on both sides of the Atlantic and effectively meet the requirements set out by EU law and the Court of Justice of the European Union.

Past TACD resolutions and statements linked to the Safe Harbour agreement:

Statements:

- TACD reaction to the announced EU-US Privacy Shield (February 2016)
- TACD Statement in Response to European Court of Justice Safe Harbour Ruling (October 2015)
- Statement of Leading Digital Rights and Consumer NGOs at the 37th International Conference of Data Protection and Privacy Commissioners (October 2015)
- TACD member organisation statements in Response to European Court of Justice Safe Harbour Ruling (October 2015)

Resolutions:

- Implementation of the Safe Harbour Agreement (May 2001)

- Safe Harbour (February 2000)
- Comments on US Department of Commerce Safe Harbour Proposal (November 1999)
- Safe Harbour Proposal and International Convention on Privacy Protection (April 1999)