Conseil des barreaux européens
Council of Bars and Law Societies of Europe
Association internationale sans but lucratif
Rue Joseph II, 40 /8 – 1000 Bruxelles
T. : +32 (0)2 234 65 10
Email : ccbe@ccbe.eu – www.ccbe.eu

CCBE Comments on the Review of the EU-U.S. Privacy Shield Agreement

25/09/2017

The Council of Bars and Law Societies of Europe (CCBE) represents the bars and law societies of 45 countries, and through them more than 1 million European lawyers.

In advance of the first annual review of the Privacy Shield in September 2017, the CCBE wishes to urge the European Commission to suspend its Implementing Decision 2016/1250 on the adequacy of the protection provided by the EU-U.S. Privacy Shield on the basis that the United States of America (U.S.) does not ensure a level of protection of personal data that is essentially equivalent to the one guaranteed by the European Union (EU).

Background

On October 6, 2015, the Court of Justice of the European Union (CJEU) issued a judgment in the case of Schrems v. Data Protection Commissioner (C-362/14) invalidating Decision 2000/520/EC on the adequacy of the protection provided by the safe harbour privacy principles.

As a result of this judgment, on 2 February 2016, the European Commission and the US Government reached a political agreement on a new framework for the transatlantic trade of personal data for commercial purposes: the EU-U.S. Privacy Shield.

The European Commission adopted on 12 July 2016 an implementing decision regarding the adequacy of the protection provided by the EU-U.S. Privacy Shield, reinforcing the need for data protection in a substantially equivalent way to that provided for by EU law. In this regard, the Commission considered the US Judicial Redress Act of 4 November 2015, which extends to EU nationals among others the guarantees granted to U.S. citizens and residents regarding the use of personal data by Federal agencies under the Privacy Act, as a substantial step forward and an important safeguard.

It should be recalled that in its declaration of 29 July 2016, the Article 29 Data Protection Working Party (WP29) expressed reservations about the Privacy Shield with regard to the access of the U.S. public authorities to data transferred from the EU. It highlighted the problems related to the lack of independence and power of the Ombudsperson, and the lack of concrete assurances prohibiting the U.S. intelligence services to carry out any massive and indiscriminate collection of personal data.

In the joined cases of Tele2 Sverige AB v. Post- och telestyrelsen (C-203/15) and Secretary of State for the Home Department v. Watson and others (C-698/15) of 21 December 2016, the CJEU gave a further indication of the restrictions legislation must impose on access to retained data in order to comply with the EU Charter of Fundamental Rights.

At the moment, the Privacy Shield is also undergoing two appeals from associations before the General Court of Justice of the EU.

CCBE concerns regarding the legitimacy of the Privacy Shield

Taking into account the standards that have been identified by the CJEU on the basis of the fundamental rights and freedoms guaranteed under EU law, the CCBE considers that the EU-U.S. Privacy Shield has a number of important shortcomings which give rise to concerns over its legitimacy, primarily regarding the lack of safeguards against wide and broad surveillance programmes of the U.S.

In this respect, reference is made to the CCBE Recommendations on the protection of client confidentiality within the context of surveillance activities (hereinafter: "CCBE Recommendations"), which were adopted on 28 April 2016. This paper sets out standards that should be upheld in order to ensure that the essential principles of professional secrecy and legal professional privilege are not undermined by practices undertaken by the state involving the interception of communications and access to lawyers' data for the purpose of surveillance and/or law enforcement. Below we shortly summarise the main CCBE concerns regarding the Privacy Shield which directly stem from these recommendations.

Lack of binding legislative control

All surveillance activities need to be regulated with adequate specificity and transparency in order to avoid the risk of arbitrary disregard for human rights.[1] In this regard, the Privacy Shield only refers to e.g. "Guidelines and Policies of the Department of Justice" or "transparent policies of the Department of Justice". As a legal basis of clear, precise and accessible rules, these policies and guidelines cannot be deemed as a form of binding legislative control. Also, the term 'national security' in the Privacy Shield is not circumscribed with adequate specificity so as to ensure that data protection infringements can be effectively reviewed in courts to ensure compliance with a strict test of what is necessary and proportionate.

Judicial and independent oversight mechanisms

Any interference with the fundamental rights to privacy and data protection should be supervised by a judicial body, which is financially and politically independent from the executive and should be irremovable, because only a judge can offer the necessary guarantees of independence. The Recommendations mentions numerous requirements[2] concerning the nature of the oversight or the mandate of the oversight body which shall be fulfilled by the oversight body before the control of the surveillance activities could be deemed satisfactory.

First, the Recommendations state that supervisory control must be entrusted to a judicial body, which is politically and financially independent form the executive branch and should be irremovable.[3] The legal framework of oversight mechanism in the Privacy Shield is multi-layered and consists of two major parts: internal and external oversight. Apparently, none of the internal oversight bodies can be financially and politically independent from the executive branch because they are basically part of it, therefore internal oversight will not fulfil the requirement of supervisory control as set out above. Under the Privacy Shield, external oversight is provided by what is said to be judicial bodies[4], including the intelligence committees of the Congress and the Privacy and Civil Liberties Oversight Board. The latter two are not judicial bodies, so the requirement of supervisory control can only be fulfilled by FISA Court. However, it should be noted that the procedure before this court is *ex parte*, meaning that the individuals concerned might not be heard, or they even might not be aware of the case.

It also has to be highlighted that the features of a given surveillance activity depends on the legal basis which is invoked when surveillance programmes are undertaken. For instance, surveillance activities carried out on the basis of Section 215 of the Foreign Intelligence Surveillance Act are almost fully subject to *a priori* judicial oversight by the FISA Court. On the contrary, the surveillance activities conducted on the basis of Executive Order 12333 are not subject to any judicial review, neither *a priori*, nor *a posteriori*.

In order to fulfil its mandate, the oversight body must be given proportionate, adequate, and binding powers by law. These competences must enable the body to make fully informed and enforceable decisions.[5] However, the Privacy Shield only specifies the rather limited competence of the Ombudsperson, and even if one considers the Ombudsperson as an oversight body (which is not made

1 CCBE Recommendations point 2.1-2.4, pages 19-20.
2 CCBE Recommendations point 4.1-.4.7, pages 22-24.
3 CCBE Recommendations point 4.2-.4.3, page 22.
4 Annex VI of The Privacy Shield invokes the Foreign Intelligence Surveillance Act Section 702.
5 Recommendations point 4.7, page 14.

clear in the Privacy Shield), it is evident that the Ombudsperson lacks any effective powers since it can only request further action by the appropriate United States Government body or request information from other governmental entities.

It also needs to be emphasized that if the supervisory body does not have at very least the power to terminate the unlawful surveillance, then that body cannot fulfil its mandate sufficiently. A supervisory body can only make enforceable decisions if it is able to order the authorities to cease and discontinue unlawful surveillance, or order the permanent destruction of information obtained through direct and indirect surveillance.

Lack of effective legal remedies

In order to provide effective legal protection against unlawful surveillance, it is necessary that legal remedies are made available to lawyers and their clients who have been the subject of unlawful surveillance. The U.S. government does not regard the protections of the U.S. Constitution, which prohibits “unreasonable” searches and seizures and imposes a warrant requirement to prevent such actions, as extending to non-U.S. persons who are outside the United States. Therefore, in the intelligence surveillance context, people in the EU who are not U.S. persons will not benefit from these constitutional protections, whereas in the EU anyone can go to court if they have a legitimate reason to suspect an interference of their fundamental rights, regardless of their citizenship.

Although the Privacy Shield highlights in general that there are both judicial and administrative remedies available to the individuals in the U.S., this has been seriously put into question by Executive Order 13768 Enhancing Public Safety in the Interior of the United States.

The Order specifically provides that the provisions of the Privacy Act will no longer apply to those “who are not United States citizens or lawful permanent residents”. The guarantees and remedies of the Privacy Act would therefore no longer benefit EU citizens who are not lawful permanent residents in the United States. Consequently, this Decree appears to over-ride the guarantees granted during the discussions on the Privacy Shield.

The Order also allows the NSA to share large amounts of personal data of non-US persons with 16 other government agencies without any mandate, court decision or authorisation from Congress.

Congress has also authorised Internet service providers to sell their subscribers' personal data, including history and other private information, without their consent.

Given that an Executive Order has a lower status than a statute in the US legal system, it could be argued that the Order of 25 January 2017 should not be regarded as calling into question the Judicial Redress Act of 4 November 2015.

However, this Order shows, at the very least (i), the intention of the American executive to reverse the guarantees previously granted to EU citizens with regard to the protection of their personal data; (ii) raises concerns that, in practice, US governmental authorities directly dependent on the executive are seeking to override the commitments made during the Obama Presidency towards the EU, and (iii) exposes EU citizens to the unauthorised use of their personal data, with no effective remedy.

In a statement on 15 February 2017, the Article 29 Data Protection Working Party indicated that it had sent a letter to the U.S. authorities requesting a clarification on the impact of this Order on the Privacy Shield. It is not known whether the U.S. authorities have replied as no answer was made public.

Jan Philipp Albrecht, the European Parliament's data protection rapporteur, was alarmed by the situation and declared: “If this is true, the EU Commission has to immediately suspend the Privacy Shield and sanction the US for breaking the EU-U.S. umbrella agreement.”

Review of the Privacy Shield

Under Article 4 of the Privacy Shield, which came into effect on 1 August 2016, an annual review of the system is foreseen.

Paragraph 5 of Article 45 of the European General Data Protection Regulation (GDPR) provides for the Commission's competence to repeal, amend or suspend its decision on adequacy "where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article."

On 12 July, Justice Commissioner Věra Jourová delivered a speech to the European Parliament Delegation for relations with the US on how to reassess the Privacy Shield. She encouraged the maintenance of the Privacy Shield, provided that the guarantees on which it was built were maintained, in particular the Ombudsperson in charge of dealing with citizens' complaints against interference by the US authorities, and the guarantees contained in the Presidential Policy Directive 28 put in place by the Obama Administration. The Commissioner did not mention the impact of the Executive Order of 25 January 2017 on the protection of European citizens' personal data.

As part of this annual reassessment, the CCBE invites the Commission to exercise its powers under paragraph 5 of Article 45 of the GDPR in order to suspend the Privacy Shield. In view of the concerns outlined above concerning the legitimacy of the Privacy Shield, it seems – in particular following the Executive Order of 25 January 2017 – that the United States no longer provides adequate protection for the personal data of EU citizens.

The renegotiation of the Privacy Shield agreement will require strong US data protection safeguards, especially as regards the access to personal data by public authorities and the US companies' certification process.