The Demise of the EU-US Privacy Shield and the Future of Personal Data Transfers from the EU

August 20, 2020 – The TMCA
by Ron Moscona

In a dramatic and widely reported decision of 12 July 2020 in the case known as *Schrems II* (*Data Protection Commissioner v Facebook Ireland Ltd*), the Court of Justice of the European Union ("**CJEU**") invalidated the decision of the EU Commission that gave legal effect in the EU to the EU-US Privacy Shield scheme. In other words, personal data transfers

Related People

- Ron Moscona

Related Capabilities

- Trademark, Copyright + Advertising
- Intellectual Property Litigation

from the EU to the US can no longer be lawfully undertaken in reliance on the scheme.

Intelligence services surveillance powers and the privacy of EU citizens

The decision follows a previous judgment of the same court in the same case from October 2015 (known as *Schrems I*) in which the Safe Harbor scheme, a predecessor of the EU-US Privacy Shield, was also invalidated by the Court.

Both decisions proceeded on the same basis, that is, that electronic surveillance programs operated by the US intelligence services under US legislation and under Presidential Executive Orders do not provide legal redress (or at least do not provide sufficient legal redress) to EU citizens whose data may be accessed unlawfully. Therefore, it was held, the schemes, which were designed to allow the free flow of personal data between the EU and the US for participating organisations, did not meet the requirements under EU law to ensure that data subjects have equivalent legal protection to their privacy rights in the US as they have in the EU.

In part, the finding of insufficient judicial redress is based on the Court's conclusion that the constitutional protection provided in the US Constitution under the 4th Amendment (in relation to unlawful searches and seizures) is effectively only available to US individuals, whereas an EU citizen (or resident) is unlikely to have standing in a US court. Further, some of the surveillance programs are based on Executive Order 12333, which provides no judicial redress at all.

So, can data still be transferred lawfully to the US?

The decision of the CJEU raises many interesting questions but it is now a political matter for the EU and the US to resolve. In the meantime, the practical question for enterprises and institutions that rely on the flow of personal data from the EU to the US (and indeed to other countries) is how to ensure that such data flows are not disrupted.

Most companies and organisations do not rely on the EU-US Privacy Shield, as the likelihood of its invalidation by the CJEU has been long anticipated. Many rely instead on the "Standard Contractual Clauses" ("**SCCs**") that have been approved by the EU Commission in a series of decisions as a lawful basis for transferring personal data to countries outside the EU.

The Court in *Schrems II* rejected a challenge to the validity of the EU Commission's decisions adopting the SCCs. However, it does not follow from the decision by any means that the transfer of personal data in reliance on the SCCs remains lawful. In fact, the decision throws serious doubts on that question.

The implications of the CJEU's decision in respect of the use of SCCs are very uncertain. What is clear is that it is the responsibility of the parties to the data transfer (the data controller who transfers the data from the EU and the party that receives the data outside the EU under the terms of the SCCs), and the responsibility of national privacy regulators in the EU member state from where the data is transferred, to ensure that the SCCs

provide adequate protection to the privacy rights of the data subjects.

It is also clear from the Court's decision that to ensure adequate protection, the SCCs (together with any additional safeguards that may be put in place) must guarantee that the level of protection that data subjects have in relation to the use of their personal data outside the EU must be equivalent to the protection they enjoy under EU law.

The Court made the point very clearly that the SCCs – which naturally do not bind national intelligence authorities in the US – cannot guarantee that personal data that is transferred to the US will not be subjected to surveillance powers without adequate judicial redress to EU data subjects. However, the Court did not say that this means that the SCCs necessarily cannot provide a lawful basis for transferring data to the US.

In what circumstances the SCCs can still provide the lawful basis for data transfers and what other "safeguards" can be put in place to ensure that data subjects enjoy an equivalent level of protection for the privacy rights are questions that were left unanswered by the Court.

What is the risk and what can be done about it?

The current position as a result of the decision in *Schrems II* is rather extraordinary.

EU legislation authorised the EU Commission to adopt the SCCs as a framework for lawfully transferring personal data to countries outside the EU that do not provide an adequate level of protection to privacy rights. The CJEU has determined that the decisions of the EU Commission adopting the SCCs were valid. However, at the same time, the Court held that the transfer of data in reliance on the SCCs may still be unlawful, and it is down to the parties to the transfer (and to national authorities) to determine whether the conditions are met for ensuring the transfer is lawful.

For any company based in the EU this is a highly unsatisfactory position. An organisation may have to make the difficult choice between suspending all data transfers to the US (and to other countries where national authorities may have surveillance powers without giving EU citizens sufficient legal redress), which could have serious economic consequences, or taking the risk that continuing such transfers might be held unlawful. The organisation could be open to regulatory action, investigations and legal claims by data subjects and regulators and it could risk significant potential penalties, injunctions and damages claims by data subjects.

Organisations that rely on data transfers between the EU and the US will have to develop strategies to avoid or minimise the risk.

Some may take the view that as long as national authorities in the relevant member state do not adopt a decision (in general or in specific cases) holding that the transfer of data in reliance of the SCCs is unlawful, it is reasonable to continue to rely on the SCCs. After all, they are based on valid decisions of the EU Commission. It should be noted in this regard that it has been reported that some national regulators (including in Germany and

Ireland) have already expressed the view that data transfers to the US under the SCCs should probably no longer be treated as lawful given the rationale of the decision of the CJEA.

A more cautious approach may require carrying out a risk assessment and putting in place additional safeguards to the SCCs. The CJEU did not indicate what these safeguards might be. It only pointed to the fact that the relevant provisions of GDPR make reference to such “appropriate safeguards”. Until some guidance emerges, it is for each organisation in each case to consider what additional measures can be put in place, given the circumstances and the assessment of the risk of the transfer in each specific case. Such safeguards can include, for example, encryption and anonymisation of data, introducing additional contractual provisions, procedures and warranties or additional diligence that would at least minimise the risks of data being exposed to surveillance by national intelligence authorities.

Finally, organisations can seek to rely on a set of derogations under the GDPR to the rule that restricts the transfer of personal data to countries outside the EU. These derogations include, among others, transfers made with the explicit consent of the data subject, transfers that are required for the performance of contractual obligations and transfers required for the establishment, exercise or defence of legal claims. For many good reasons, organisations historically tended not to rely on those derogations as a sole basis for international transfers of data. Following *Schrems II*, however, the SCCs can no longer be considered an entirely safe legal route and so in appropriate circumstances it may be better to rely on those derogation.