Snowden Aftershocks: High Court Invalidates U.S. - EU Safe Harbor

Barbara E. Hoey

October 13, 2015

To our readers:

I wanted to share this insightful post from my partner and Privacy expert Alysa Hutnik concerning the recent decision by the European Court of Justice in the *Maximillian Schrems v Data Protection Commissioner* case, which effectively invalidated the Safe Harbor rule which had allowed US companies to safely share employee data among subsidiaries here and in the EU. As Alysa outlines, this decision creates huge uncertainty and arguably requires employers to create model contracts, or corporate rules to allow for such international data sharing. The Secretary of Commerce issued a statement last week expressing that she was "deeply disappointed" with the decision, and promising the issuance of an updated Safe Harbor framework "as soon as possible."

Stay tuned here and to our Privacy blog for further developments.

.....

This week, largely driven by concerns over indiscriminate U.S. surveillance of EU citizen data, the Court of Justice of the European Commission (ECJ) invalidated the 15-year-old U.S.-EU Safe Harbor framework in *Maximillian Schrems v Data Protection Commissioner*. The Court found that each EU Member State has the right to determine for itself whether a data transfer provides an adequate level of protection and thus whether data about their citizens can be transferred to the U.S.

In short, the ECJ determined that:

1. The U.S.-EU Safe Harbor framework is invalid because:

- The U.S.-EU Safe Harbor framework enables the U.S. government and other public authorities to broadly access EU citizens' data;
- Those EU citizens lack legal remedies to seek access to their data obtained in this manner or to obtain the rectification or erasure of such data; and
- These deficiencies do not provide a level of protection of fundamental rights that are equivalent to those guaranteed within the EU.

2. National data protection authorities (DPAs) have the power to investigate the transfer of data to a non-EU country to determine whether there is "adequate protection," even if the data transfer at issue is subject to a company's safe harbor certification.

Brief Background:

The European Commission's (EC) Directive on Data Protection, Directive 95/46/EC, went into effect in October 1998, and prohibits the transfer of personal data to non-EU countries that do not meet the EU's "adequacy" standard for privacy protection. In 2000, the Department of Commerce in consultation with the EC developed a "safe harbor" framework, whereby companies could transfer personal data concerning a EU citizen to the U.S. if the company self-certifies to the U.S.-EU Safe Harbor Framework. In Decision 2000/520/EC, the EC determined that there is an adequate level of protection for transferring data from the EU to the U.S., if entities comply with the Safe Harbor privacy principles.

Max Schrems, an Austrian Facebook user, filed a complaint with the Irish DPA, alleging that the transfer of data from Facebook Ireland to Facebook USA should cease because the U.S. does not ensure an adequate level of protection under the Safe Harbor. The Irish DPA determined that it would not investigate the complaint on the grounds that it was "unsustainable in law" and cited to Decision 2000/520/EC. Schrems filed an action before the Irish High Court. That court stayed the proceedings and referred the following questions to the ECJ for a preliminary ruling determining whether a DPA is bound by Decision 2000/520/EC or if it could conduct its own investigation into the adequacy of the country's data protection.

Next Steps for Companies that Relied on Safe Harbor:

The ECJ's decision means that, for the more than 4500 companies that currently rely on the U.S.-EU Safe Harbor to transfer EU individual data to the U.S., they now will need to assess alternative compliance methods for addressing international data transfers, or face potential legal exposure in Europe. Alternative compliance options include model contracts, binding corporate rules, or by obtaining individual consent. But none of these are a small effort or can be done relatively swiftly.

That quandary is causing headaches for many businesses, aware that the EC decision is effective immediately. At the very least, DPAs collectively will be issuing guidance for businesses that should be helpful in assessing the practical implications of the ECJ decision and considerations and timing for obtaining new compliant data transfer mechanisms. For example, should pre-existing model contracts be updated to address the U.S. surveillance concerns discussed in the ECJ decision? If a Safe Harbor 2.0 is adopted in response to the ECJ decision, will there still be uncertainty on whether to rely on it if individual DPAs can still scrutinize and question if there is adequate protection?

In the meantime, here's what the White House, the FTC, and Commerce had to say. More to come as we follow the developments...