October 6, 2015

Weil

Alert
Cybersecurity, Data Privacy & Information Management

Need For A "Safer" Safe Harbor Following the ECJ's Schrems Ruling

By Randi Singer, Barry Fishley, and Britta Grauke

On October 6th, 2015, the European Court of Justice (ECJ) issued a ruling in *Schrems v. Data Protection Commissioner* that has invalidated the European Commission's decision that the data privacy principles of U.S.-E.U. Safe Harbor — pursuant to which U.S. companies transfer personal information about E.U. citizens to the U.S. after agreeing to abide by these principles — provide an adequate level of protection for the data of E.U. citizens. As a result of this ECJ decision, the privacy supervisory authority in each E.U. Member State has the power to question whether transfers of personal data to the U.S. comply with E.U. data protection law and to suspend such transfers if E.U. privacy obligations are not met. The impact is potentially enormous for the thousands of U.S. multinational companies that currently operate under the Safe Harbor (as well as for the thousands of European businesses that have their data hosted in the U.S. by these U.S. companies), but the European Commission has indicated that it is committed to finding a "safer" safe harbor so that the transfer of transatlantic data can continue. Regardless, companies that rely on the U.S.-E.U. Safe Harbor agreement must review their current practices and consider alternatives.

Background

European data privacy law prohibits the transfer of personal data to a country outside the European Economic Area unless that country ensures an adequate level of protection for individuals' personal data. In order to enable U.S. organizations to comply with this European law, the U.S. Department of Commerce worked with the European Commission to develop a "Safe Harbor" framework, which allowed U.S. organizations that self-certified compliance with the safe harbor principles (which are similar to E.U. data protection principles) to transfer data concerning E.U. citizens to the U.S. The ECJ has now ruled that the Safe Harbor scheme is invalid and that any E.U. Member State's national supervisory authorities may question whether a transfer of personal data to the U.S. complies with E.U. data privacy laws, despite reliance on the scheme.

Procedural History

Schrems originated as a lawsuit brought by Austrian privacy activist Maximillian Schrems in Ireland. In light of the 2013 Edward Snowden disclosures concerning the NSA and U.S. electronic surveillance, Schrems filed a complaint with the Irish Data Protection Commissioner arguing that his personal data, some of which is transferred from Facebook's Irish subsidiary to Facebook's U.S. servers, is not adequately protected under the current Safe Harbor regime.[1] The Data Protection Commissioner rejected the complaint, in part because of reliance on the Safe Harbor scheme which the European Commission had decided provided adequate protection to E.U. citizens. Upon judicial review, the High Court of Ireland asked the ECJ to clarify whether the Safe Harbor agreement prevented a national data protection authority (DPA) from investigating a complaint alleging that a third country (i.e., the U.S.) does not ensure an adequate level of protection, thereby allowing the suspension of data transfers.

In his September 23, 2015 opinion, Advocate General Yves Bot found that the Safe Harbor agreement did not ensure adequate protection of E.U. users' personal data transferred to the U.S. Further, the Advocate General argued that data protection authorities of Member States had the obligation to protect the personal data of all E.U. citizens. Notwithstanding the Safe Harbor agreement, Bot wrote that the data protection authorities of an individual Member State should be able to suspend the transfer of data of E.U. users to servers located in the U.S., which would effectively undermine the Safe Harbor agreement. Advocate General Bot's opinion intimated that the ECJ could and should require the European Commission to invalidate the Safe Harbor agreement.[2]

The ECJ Decision Summary

On October 6th, 2015, the ECJ issued a non-appealable opinion that essentially invalidates reliance upon the U.S.-E.U. Safe Harbor. Adopting the reasoning of the Advocate General's Opinion, the ECJ found that Safe Harbor did not provide an adequate level of data protection given U.S. intelligence activities. The ECJ held that the European Commission's 2000 decision finding that the U.S. Safe Harbor provides an adequate level of protection is invalid and does not trump the powers available to E.U. national data supervisory authorities to question the lawfulness of transfers under the U.S. Safe Harbor regime.[3]

The *Schrems* case will resume in Ireland, with the specific merits of that case to be determined. As a result of the ruling, we are likely to see other data privacy complaints filed against DPAs in other Member States, with unpredictable and likely varying results. Thus, the privacy requirements in the E.U. have the potential to become disparate and unwieldy, and U.S. companies may find it necessary to adjust their data privacy policies on a country-by-country basis.

Takeaways

We expect that E.U. national data supervisory authorities will be inundated with complaints from individuals and consumer groups. There are a number of existing alternatives to the Safe Harbor, which include:

- Restructuring data storage architecture to ensure that European data remains in Europe. Such a restructuring may add significant cost as well as impacting corporate structure.
- Adopting Binding Corporate Rules (BCRs), which are internal rules adopted by multinational groups of companies and approved by the E.U.[4] BCRs

can be costly and time consuming to develop and implement, but would provide a U.S. company with essentially the same capacity to transfer data as it enjoyed under the Safe Harbor agreement.

- Adopting the pro forma model contractual clauses approved by the European Commission.
- Obtaining individual consent. For example, the addition of an extra consent form for European users to click, explicitly allowing a company to transfer their data to U.S. servers.

In the wake of the decision, the European Commission has said it would work with national supervisory authorities to issue further guidelines – including a "safer" safe harbor. European Commission and U.S. officials had already entered into negotiations in 2013 for creating a new Safe Harbor agreement. The ECJ ruling may also place more pressure on Congress to pass legislation currently under consideration that would allow E.U. citizens to bring privacy lawsuits in U.S. courts.

---

1. European Court of Justice Press Release No 106/15, Advocate General's Opinion in Case C-362/14 *Maximillian Schrems v. Data Protection Commissioner* (Sept. 23, 2015).
2. *See id.*
3. European Court of Justice Press Release No 117/15, Judgment in Case C-362/14 *Maximillian Schrems v. Data Protection Commissioner* (Oct. 6, 2015).
4. *European Commission's Directorate General for Justice and Consumers, Overview on Binding Corporate Rules* (Sept 2, 2015), available at http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm

Cybersecurity, Data Privacy & Information Management is published by Weil, Gotshal & Manges LLP, 767 Fifth Avenue, New York, NY 10153, +1 212 310 8000, www.weil.com.

If you have questions concerning the contents of this issue, or would like more information about Weil's Cybersecurity, Data Privacy & Information Management practice, please speak to your regular contact at Weil, or to the editors or authors listed below:

Editors:

Michael Epstein (NY)	Bio Page	michael.epstein@weil.com	+1 212 310 8432
Randi Singer (NY)	Bio Page	randi.singer@weil.com	+1 212 310 8152
Paul Ferrillo (NY)	Bio Page	paul.ferrillo@weil.com	+1 212 310 8372

Contributing Authors:

Randi Singer (NY)	Bio Page	randi.singer@weil.com	+1 212 310 8152
Barry Fishley (London)	Bio Page	barry.fishley@weil.com	+44 20 7903 1410
Britta Grauke (Frankfurt)	Bio Page	britta.grauke@weil.com	+49 69 21659 664