October 6, 2015

ECJ Safe Harbor Opinion Has Implications for all Data Transfers out of Europe

By Miriam H. Wugmeister

Today The European Court of Justice (ECJ) followed the core of the Opinion of the Advocate General (AG) (see our Privacy Minute dated October 3, 2015) in *Schrems v. Data Protection Commissioner* (Case No. C-362/14).

SUMMARY

In sum, the ECJ held that:

1. Member State Data Protection Authorities (DPA) must be allowed to:
    - examine complaints from individuals regarding the treatment of their personal information by other countries;
    - bring cases to court to question the validity of adequacy decisions; and
    - suspend the transfer of personal information to other countries when they believe it is appropriate.
2. The Safe Harbor Decision is invalid because:
    - US companies may provide information to the US government to protect national security, public interest or law enforcement requirements;
    - The US does not provide European individuals with the ability to obtain judicial redress in the US; and
    - The European Commission overstepped its authority by limiting the bases on which DPAs could suspend transfers to the US.

IMPLICATIONS:

This decision opens the door for every DPA to evaluate whether other countries outside the EU provide adequate protection for personal information. The Standard Contractual Clauses (SCCs) specifically give the DPAs the authority to prohibit or suspend transfers to other countries when the DPA determines that the laws of the other country are insufficient to protect privacy. Similarly, the adequacy decisions for Switzerland, and Canada and Argentina all provide authority for the

UNITED STATES

California

Tiffany Cheung	(415) 268-6848
Rebekah Kaufman	(415) 268-6148
Christine E. Lyon	(650) 813-5770
David F. McDowell	(213) 892-5383
Purvi G. Patel	(213) 892-5296
Andrew Serwin	(858) 720-5134
Stephanie Sharron	(650) 813-4018
David M. Walsh	(213) 892-5262

New York

Melissa Crespo	(212) 336-4354
John F. Delaney	(212) 468-8040
Michael B. Miller	(212) 468-8009
Suhna N. Pierce	(212) 336-4150
Marian Waldmann Agarwal	(212) 336-4230
Miriam H. Wugmeister	(212) 506-7213

Washington, D.C.

L. Richard Fischer	(202) 887-1566
Adam J. Fleisher	(202) 887-8781
Libby J. Greismann	(202) 778-1607
Julie O'Neill	(202) 887-8764
Cynthia J. Rich	(202) 778-1652
Nathan David Taylor	(202) 778-1644

EUROPE

Berlin

Hanno Timner	49 30 72622-1346
Lokke Moerel	44 20 79204054

Brussels

Karin Retzer	32 2 340 7364
Sotirios Petrovas	(212) 336-4377
Alja Poler De Zwart	32 2 340 7360
Ronan Tigner	32 2 340-7358

London

Alex van der Wolk	44 20 79204074
Alistair Maughan	44 20 79204066
Daniela Guadagno	44 20 79204024
Sarah Wells	44 20 79204167

ASIA

Beijing

Paul D. McKenzie	86 10 5909 3366
Wei Zhang	86 10 5909 3366

Hong Kong

Gordon A. Milner	852 2585 0808

Singapore

Daniel P. Levison	65 6922 2041

Tokyo

Toshihiro So	81 3 3214 6568
Kyoko Sato	81 3 3214 6936
Yukihiro Terazawa	81 3 3214 6585

DPAs to suspend transfers to these countries. Thus, the ultimate effect of the ECJ decision is to remove certainty and disrupt harmonization across the European Union and allow each DPA to decide for itself what cross-border transfers are permissible.

Moreover, because the invalidation of the Safe Harbor Decision was based, at its core, on a finding that the US does not provide adequate protection for personal information, that same logic can be applied to every other adequacy mechanism such as Binding Corporate Rules (BCRs) and the SCCs. Thus, a second result of the decision is that none of the existing adequacy mechanisms is a safe bet at the moment because the DPAs now have authority to independently determine if the recipient country, such as India, Brazil, China or the U.S., provides appropriate security (independent of the adequacy mechanism).

This decision demands a political solution that addresses the following points:

- The EU and the US must agree on what protections will be sufficient to protect personal information. It is worth noting that on September 8, 2015, the EC and the U.S. agreed on privacy safeguards to govern the exchange of personal information in the context of cooperation between law enforcement agencies. If the safeguards that the U.S. and the EC are willing to implement are adequate in the context of direct sharing of personal information between law enforcement authorities, surely those safeguards should also be adequate when U.S. companies transfer data to law enforcement. By not agreeing to these safeguards at the appropriate governmental level, companies are forced to either violate the European data protection rules and share the personal information as lawfully ordered by U.S. authorities, or they can refuse to share the information and be at risk of penalties for not responding to a lawful request from the U.S. government. This type of catch 22 situation will not be solved under the draft Data Protection Regulation. The issue will only be exacerbated as violations of the European privacy rules will carry the risk of a fine of 2% of a company's global revenues.
- A consensus must be reached within Europe regarding whether harmonization is a priority and how important having a single market for the sharing of data will be.

PRACTICAL IMPLICATIONS FOR COMPANIES

Companies have only a series of bad choices before them:

- They can take steps to immediately substitute another adequacy mechanism for the Safe Harbor such as BCRs or SCCs. This, however, will leave them entirely vulnerable to any DPA taking the position that the recipient country does not provide adequate protection and thus suspending or prohibiting the transfer based on those other mechanisms.
- Companies could state that they will not allow any government access to personal information received from Europe and then potentially place themselves at risk of ignoring a valid government request such as a subpoena or court order.
- Companies could elect to seek consent from all individuals whose information is collected in Europe, which in many circumstances is expensive, difficult and impractical (and is often a problem for employee data).

In a press conference today, the European Commission stated that it perceives the ECJ's ruling as confirming the Commission's approach to the renegotiation of the Safe Harbor and that, in the meantime, transatlantic data flows can

continue using other mechanisms available or exceptions provided for under EU law (e.g., performance of a contract, public interest, consent). The Commission intends to work closely with national DPAs and will issue "clear guidance" on how to deal with data transfer requests to the US in light of the ruling, to avoid a patchwork of contradictory decisions. While reiterating the importance of protecting personal data, the Commission set as a priority to ensure that data flows can continue, as they are the "backbone" of the EU economy.

Just as with the whistleblowing hotlines a few years ago, the ECJ opinion has brought into clear view the conflict of laws between Europe and the US. Companies may spend a tremendous amount of time and money in the next few weeks seeking an alternative which just does not exist.

Waiting to see how this settles in the next few weeks may be the wisest course of action.

About Morrison & Foerster:

We are Morrison & Foerster — a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer's A-List* for 11 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Morrison & Foerster has a world-class privacy and data security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by *Chambers* and *Legal 500* as having one of the best domestic and global practices in this area.

For more information about our people and services and the resources we offer such as our treatise setting out the U.S. and international legal landscape related to workplace privacy and data security, "*Global Employee Privacy and Data Security Law,*" or our free online Privacy Library, please visit our practice page and follow us on Twitter @MoFoPrivacy.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.