No More “Safe Harbor” for the EU-US Transfer of Personal Data - Is Your Online Business Endangered?

October 7, 2015

What Happened? The highest court in the European Union, the EU Court of Justice, has just invalidated the EU-U.S. Safe Harbor mechanism. Companies can no longer rely on Safe Harbor certification to justify data transfers of EU personal information to the U.S.

So What? The EU or its constituent member nations can now stop data transfers or levy fines upon finding that a U.S. business or its cloud provider has violated its jurisdictional privacy requirements.

What Should Your Business Do? All businesses on U.S. soil should take a close look at how they process, store and transfer the personal data of EU citizens. Cloud providers are going to have to explain to their customers and EU authorities how they can protect EU personal data from falling within the reach of the U.S. intelligence and law enforcement community.

How Did We Get Here? In 2011, Max Schrems was an Austrian study-abroad student in Professor Dorothy Glancy's Privacy Law course at Santa Clara University School of Law. After a Facebook privacy lawyer spoke to the class, Schrems began a term paper based on his view that Facebook lacked awareness of European privacy law.

Schrems asked Facebook for his data going back to the 2008 start of his account. Facebook sent him a CD with more than 1,200 pages of data. It had messages, status updates, wall posts and other information he thought he had deleted. It contained a log of his "last locations," apparently gleaned from his check-ins, data gathered from apps, IP addresses and geo-tagged uploads. It even held email addresses from his friends' address books, which he had never provided. Schrems brought a privacy claim under EU law against Facebook Ireland, which had transferred the data to the U.S. He contended that the U.S. allowed too much government access to his data.

What Did the EU Court Decide? The EU Court of Justice invalidated the Safe Harbor program because it found that current U.S. data protection compromises "the essence of the fundamental right to respect for private life." It remanded the case to the Irish High Court to determine "whether the transfer of the data of Facebook's European subscribers to the United States should be suspended on the ground that that country does not afford an adequate level of protection of personal data." *Maximillian Schrems v Data Protection*

Commissioner, Case C-362/14, ECR [2015] (delivered Oct. 6 2015).

What's Next? More than 4,000 companies have been using the EU-U.S. Safe Harbor protocol to transfer EU citizens' personal data to the U.S. The Federal Trade Commission has administered and enforced the program, in which companies self-certify as compliant with EU data protection standards. See https://www.ftc.gov/tips-advice/business-center/guidance/information-eu-residents-regarding-us-eu-safe-harbor-program.

The *Schrems* decision should not come as a surprise. The EU and its members have been highly critical of Safe Harbor even before Edward Snowden revealed the extent to which the NSA was seeking information from Google, Yahoo and others. For example, in February 2015, the German states of Berlin and Bremen each began company investigations on the grounds that Safe Harbor certification alone did not satisfy EU data protection standards.

The EU and United States have been attempting to renegotiate the Safe Harbor framework for some time. This court decision should motivate progress in their talks. They have recently developed a working "umbrella" process for transfer of personal data between governments.

With Safe Harbor gone, American and multinational companies can still attempt to rely on pre-approved Model Contract Clauses and internal Binding Corporate Rules to transfer the data to the U.S., but these alternatives have significant drawbacks and are now likely subject to stricter scrutiny by EU Data Protection Authorities.

Finally, the EU Commission is considering a new General Data Protection Regulation that would create a "one-stop shop" for EU data regulation. At the same time, however, the GDPR proposes huge fines for violation of the new regulation: €1,000,000 [about $1,127,450] or up to 5 percent of an enterprise's "annual worldwide turnover," whichever is greater.

The future will bring more interplay between U.S. and foreign law, as the world gets smaller and more economically interdependent. Last month, U.S. Supreme Court Justice Stephen Breyer released a book on this topic, *The Court and the World: American Law and the New Global Realities*. International data transfer is one of those new global realities.