Lowndes

Insights

Europe's Top Court Decision May Halt Trillion Dollar U.S. Data Transfer Business Partnership with EU

Lowndes Tech Blog
09.14.2020

Related Attorneys

James O'Brien

Related Expertise

Intellectual Property

Technology

In today's rapidly evolving global economy, data is king. Whether we're talking about blockchain, analytics or how much your online shadow personality is being sold for, there is no doubt that there is an incredibly lucrative market for gathering, storing and selling data. In fact, influential companies like Facebook transfer data across the Atlantic Ocean as part of a $7.1 trillion transatlantic economic partnership between Europe and the U.S.

While Facebook must have been thrilled about the revenues related to its data business, a privacy activist and lawyer residing in Ireland, Max Schrems, was much less giddy about his data being used as a cash cow at the expense of his privacy. Mr. Schrems decided to throw a wrench in things when he filed a complaint that found its way to the highest court in Europe, leading to a legal decision recently issued that will inevitably affect not just the economics of the transatlantic partnership and other countries moving data in and out of Europe, but may also affect U.S. security, surveillance and defense laws.

To understand the European Court's decision, we must understand the general context of the legal landscape created by the European Union's law known as GDPR (General Data Protection Regulation). The GDPR is a set of stringent European data privacy laws effectively recognizing privacy as a fundamental human right by creating mechanisms whereby consumers and governments can and, at times, must take action to ensure the privacy of European citizens' data. Of particular importance to this discussion is the requirement stating that if an EU citizen's data is being transferred out of the EU, the country to which the data is being transferred must afford roughly equal protection as consumers would have under the GDPR.

Facebook has been transferring large sets of data from Europe to the U.S., and Mr. Schrems did not feel the U.S. privacy standards were good enough for the U.S. to play in the Euro league. In other words, Mr. Schrems felt the U.S. prioritization of its national defense created a pervasive culture of surveillance that should preclude companies like Facebook from

transferring data from the EU to the U.S. under the data transfer mechanism via EU-U.S. Privacy Shield Framework designed by U.S. Department of Commerce, and the European Commission (Privacy Shield). The European Court of Justice agreed and invalidated the Privacy Shield based upon inadequacy of protection.

The European Court did not specifically invalidate all data transfer mechanisms currently in use (a mechanism called SCC survived the decision). However, the court's decision effectively told companies and regulatory bodies in the EU that the U.S. surveillance laws violate the principles of EU privacy rights and do not currently provide EU citizens with privacy protection required under the GDPR. The scope and practical implications of this decision are sure to set off some fireworks in the near future as we have now seen the first private lawsuits filed in Europe in the form of class action suits brought against Oracle and Salesforce.

Everyone agrees that companies will have to take a critical look at their data transfer and retention policies to conform to this new and ever-evolving legal landscape, but there is certainly tension and dispute about the benefit, scope, and implications of the European Court of Justice's impactful decision. U.S. government officials are not happy about essentially having to choose between revamping national security and surveillance laws to implement pragmatic privacy protections or taking a massive hit to the U.S. economic transatlantic data partnership with benefits in the trillions. But those officials are not getting any sympathy from Mr. Schrems who said, "This judgment is not the cause of a limit to data transfers, but the consequence of U.S. surveillance laws. You can't blame the Court to say the unavoidable — when $#@! hits the fan, you can't blame the fan."

A link to the full CJEU judgement can be found here.