MONDAY, AUGUST 17, 2020 | SERVING CHICAGO'S LEGAL COMMUNITY FOR 164 YEARS | CHICAGOLAWBULLETIN.COM

Chicago Daily Law Bulletin®

VOLUME 166, NO. 125

LAW BULLETIN MEDIA

Piercing the shield: Eliminating the European Union privacy shield

We will return to the Supreme Court and rule of law in future columns. But, for the next few columns, we will be focusing on some issues that have developed in privacy and cyber. This week, we review the invalidation of the Privacy Shield.

Safe Harbor

In 2000, the European Commission (EC) introduced safe harbor. It was a method to address the findings by the European Union ("EU") that United States privacy regimes and frameworks were not adequate or equivalent to the EU framework. It was a principles-based, voluntary framework to allow companies to transfer personal data of European residents to the U.S. Austrian law student Maximilian Schrems took Facebook to court claiming that, once his data reached U.S. soil, privacy protection faded and sought that the safe harbor be invalidated.

Five years later, the European Court of Justice (ECJ) declared it invalid. To replace it in 2016, the EC issued the EU-US Privacy Shield. The new framework was supposed to provide additional protection to EU citizens' data with the creation of new safeguards, such as the data protection ombudsman, and the "promise" that U.S. surveillance would be limited.

On July 16, the European Commission deemed the EU-U.S. Privacy Shield Framework adequate to enable data transfers under EU law. The privacy shield had replaced the prior safe harbor. The new framework was supposed to provide additional protection to EU citizens' data with the creation of new safeguards, such as the data protection ombudsman, and the "promise" that U.S. surveillance would be limited.

In July, the ECJ decided that these expectations have not been met and invalidated the privacy shield.

In July, the ECJ decided that these expectations have not been met and invalidated the privacy shield. In Schrems II, ECJ concluded that the Standard Contractual Clauses (the "SCCs") issued by the European Commission for the transfer of personal data to data processors established outside of the EU are valid, but it struck down the privacy shield framework on the basis that the limitations on U.S. public authorities' access to EU personal data were not sufficient for the level of protection in the U.S. to be considered equivalent to that ensured in the EU, and that the framework does not grant EU individuals actionable rights before a body offering guarantees that are substantially equivalent to those required under EU law.

The U.S. and EU need to go back to the drawing board to determine if there is a framework that would pass muster and that Schrems would not successfully challenge. On August 10, the EU Commissioner for Justice Didier Reynders and Secretary of Commerce Wilbur Ross issued a joint press statement, providing in part:

"The U.S. Department of Commerce and the European Commission have initiated discussions to evaluate the potential for an enhanced EU-U.S. Privacy Shield framework to comply with the July 16 judgment of the Court of Justice of the European Union in the Schrems II case. "

COTTER'S CORNER

DANIEL A. COTTER

DANIEL A. COTTER *is a partner at Howard & Howard Attorneys PLLC and author of the book "The Chief Justices" (Twelve Tables Press). The views expressed here are solely those of the author. He can be reached at scotuslyyours@gmail.com.*

About 5,000 companies currently rely on the privacy shield framework to transfer personal data to the U.S. The invalidation of the privacy shield potentially has a significant impact on those companies, many of whom have self-certified. Shortly after the invalidation, the website, maintained by the United States Department of Commerce, updated the information about the framework (emphasis in original):

On July 16, the Court of Justice of the European Union issued a judgment declaring as "invalid" the European Commission's Decision (EU) 2016/1250 of 12 July 2016 on the adequacy of the protection provided by the EU-U.S. Privacy Shield. As a result of that decision, the EU-U.S. Privacy Shield Framework is no longer a valid mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States. This decision does not relieve participants in the EU-U.S. Privacy Shield of their obligations under the EU-U.S. Privacy Shield Framework.

The U.S. Department of Commerce will continue to administer the Privacy Shield program, including processing submissions for self-certification and re-certification to the Privacy Shield Frameworks and maintaining the Privacy Shield List. If you have questions, please contact the European Commission, the appropriate European national data protection authority or legal counsel.

For companies previously relying on the Privacy Shield, there are various ways to proceed forward. Businesses in the EU that export data into the U.S. (including those that work with data processors in the U.S.) can still use the SCCs for these transfers.

Additionally, the GDPR (Articles 45 and 49) provides additional transfer mechanisms, including binding corporate rules, explicit consent from data subjects for each transfer, or when the transfer is necessary for the performance of a contract with the data subject. Companies that relied on the

Privacy Shield as their best option, especially businesses in the U.S. that collect data directly from EU consumers, will likely need to reconsider transfer mechanisms they rejected in favor of the Privacy Shield. Until such time as a replacement for the Privacy Shield is negotiated, these options should be considered to ensure that EU-U.S. data transfer remains compliant with applicable European laws and regulations, including the GDPR.

To keep these vital transfers flowing while complying with the ECJ's ruling, companies should continue to self-certify, and should also take additional steps:

- Map out data transfers.
- Assess alternatives and adopt the SCCs with caution. SCCs have become the go-to strategy for most companies, and the ECJ affirmed their validity, with some indications that they might be changing and also that more scrutiny might be placed on the adherence to the SCCS going forward.. These may be changing soon.
- Review third parties' data flows and contracts.

Conclusion

The recent decision by the ECJ calls attention and focus to the privacy protection laws and rules in the United States and whether they are adequate. The shield has been pierced.