

OCTOBER 7, 2020



The once-and-future Privacy Shield (?)

By Jason Gonzalez, Jenny Holmes, and Troy Lieberman

The European Court of Justice's July 2020 invalidation of the Privacy Shield threw much of the international business world into panic and confusion, given that over 5,300 companies—and trillions of dollars of US-EU trade—had been relying on the Privacy Shield to validate data flows between the US and the EU. Unfortunately, the last few months have done little to set things right again. This alert provides a summary of where things stand now, and potential ways forward for the future.

A quick review...

On July 16, 2020, the ECJ issued an opinion in a lawsuit brought by former law student Maximillian Schrems against Facebook. In its July ruling, now referred to as the “Schrems II” opinion, the ECJ determined that the Privacy Shield was invalid. According to the ECJ, the Privacy Shield—the mechanism negotiated by the US and EU, by which companies could self-certify that their data protection protocols provided sufficient protection to EU data—could not stand due to the fact that, no matter what the self-certifying companies said, the US government’s national security surveillance practices were too intrusive, and provided no effective means of redress for affected EU data subjects. While the Schrems II opinion left the “Standard Contractual Clauses” (“SCCs”) data transfer mechanism intact, it did say that companies relying on them must be ready to justify, on a case-by-case basis, how the particular data flow covered by the SCCs offers EU data subjects sufficient protection against the surveillance concerns.

So how do things stand currently? Unfortunately, mostly unsettled:

No enforcement “Grace Period,” nor any “new-and-improved” Privacy Shield on the horizon

As some may recall, back in 2015 the Schrems-Facebook case yielded an earlier blockbuster ruling—the invalidation of the “Safe Harbor,” which was the US-EU data transfer method that preceded the Privacy Shield. Shortly after the Safe Harbor was invalidated, the EU authorities announced a moratorium on enforcement actions while the EU and US authorities negotiated a Safe Harbor replacement, which took over a year. After the Schrems II ruling, however, no similar enforcement moratorium has been announced, nor has any EU guidance been issued to assist companies trying to negotiate the new legal landscape. There also thus far have been no clear

indications of progress on any replacement or “improved” Privacy Shield that would address the ECJ’s Schrems II concerns.

Israel and Switzerland follow the EU’s lead

Last week, the Israeli Privacy Protection Authority announced that, for the same reasons articulated in the Schrems II opinion, the Israel-US Privacy Shield is no longer valid to protect data transfers between the two countries. In September, the Swiss Federal Data Protection and Information Commissioner reached essentially the same decision with respect to Switzerland-US data transfers.

The US response Part I—Keep following the Privacy Shield

In the days following the Schrems II decision, the US Federal Trade Commission, which administers the Privacy Shield, issued a statement saying that, despite the Schrems II decision, “[w]e continue to expect companies to comply with their ongoing obligations with respect to transfers made under the Privacy Shield Framework.” In other words, the US government (including via FTC enforcement) expects certified companies to continue to adhere to Privacy Shield standards, even if the EU no longer considers the standards a valid transfer mechanism.

The US response Part II—Supporting the SCCs

Late last week, the United States government issued a “white paper” in which it addressed the ECJ’s criticisms of the SCCs, and offered several points for companies to consider when attempting to justify particular SCCs data transfers. In brief, the white paper discusses the fact that, in the US government’s view at least, the Schrems II decision focused on aspects of US surveillance that have long ago been superseded. The white paper claims that currently there are several practical limits on US surveillance, including the fact that many US businesses are not often subject to it; that there are numerous procedural safeguards now in place that are designed to prevent surveillance abuse; and that certain US statutes in fact provide legal redress available to EU citizens affected by US government surveillance. The white paper thus, in essence, helps provide practical “cover” to businesses looking for ways to justify that their use of the SCCs is “safe” under the Schrems II standards.

What’s next?

It is difficult to reliably predict what will happen, and when, with the Privacy Shield. It is clearly the case that many businesses would like clarity and resolution as soon as possible, as would the US government, which, in conjunction with the issuance of the white paper, published an article in *Lawfare* beseeching the EU to work with the US “to provide the legal clarity and certainty essential to transatlantic commerce and cooperation.” While the European Commission has stated that revised the SCCs may be issued by the end of 2020, these revisions were in the works even before the Schrems II decision, and it is unclear at this point whether the new SCCs would be able to (or are even intended to) provide the case-by-case data flow security justifications the Schrems II decision appears to contemplate.

Given all the uncertainty, there is no risk-free easy answer on what businesses should do at this point. Many Privacy Shield-certified companies, post Schrems II, have opted to implement the SCCs as, essentially, the only remaining practical means of validating EU-US data flows. Companies using the SCCs should consider the white paper’s points and justifications, as well as other facts

specific to the company's particular data flows—including whether they are of the type typically subject to government surveillance, and whether the company has ever received any requests for information from the US government—when analyzing the security issue. Even with the SCCs in place, however, companies should consider maintaining their Privacy Shield status given that, if a new and improved Privacy Shield is eventually issued, having the current Privacy Shield in place may make the transition easier. Additionally, companies that are already certified with the Privacy Shield must continue to comply with the obligations thereunder. Regardless, with luck and continued pressure from the international business community, additional clarity and guidance hopefully will be coming soon.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

- Jason Gonzalez, 213-629-6019, jgonzalez@nixonpeabody.com
 - Jenny Holmes, 585-263-1494, jholmes@nixonpeabody.com
 - Troy Lieberman, 617-345-1281, tlieberman@nixonpeabody.com
-