

Tying it all together: Safe Harbor and Security-Related Data Flows

Article By:

Susan L. Foster, Ph.D.

One of the fascinating aspects of the privacy-related negotiations between the EU and the US over the past couple of years has been the EU's efforts to decouple trade (e.g, [TTIP](#)) and security-related negotiations from the Safe Harbor 2.0 negotiations. The US Senate's Judiciary Committee pushed back firmly on that yesterday when it adopted [amendments to the Judicial Redress Act](#), which the EU requires to be passed before it will sign the Umbrella Agreement between the US and EU relating to the sharing of crime-related information between law enforcement authorities. The [basic aim of the Judicial Redress Act](#) is to give EU citizens the same rights as US citizens under the United States' Privacy Act of 1974. The European Commission has said a number of times that passage of the Judicial Redress Act was a step in the right direction for Safe Harbor 2.0 ([without saying it was enough](#) to fully address the Commission's concerns).

The Judicial Redress Act creates a mechanism under which the Attorney General can designate a particular country as a "covered country" for purposes of its citizens rights under the Privacy Act if the country has appropriate privacy laws and actually shares information "for the purpose of preventing, investigating, detecting, or prosecuting criminal offenses." In other words, the other country needs to reciprocate the US's information sharing relating to crime – information has to flow in both directions.

The Senate Judiciary Committee added one more category for reciprocity: the transfer of personal data for commercial purposes. In other words, if the EU – or a specific EU country — bans the transfer of personal data to the US for commercial uses (for example, if the German regional DPA in Schleswig-Holstein acts on its reported [threat to ban transfers](#) to the US under the model clauses and consent, which are pretty much the only bases possible after Safe Harbor was struck down), then the US can refuse to grant the EU (or specific country) status as a "covered country." That would probably result in the Umbrella Agreement being suspended and crime-related information flows stopping – an outcome that would leave both the US and the EU more vulnerable to security threats and less able to investigate international crimes effectively.

The EU's attempts to decouple trade and security-related negotiations from the questions around transfers of personal data by the business sector seem finally to have foundered on the hard rocks of scrutiny during the US legislative process. It remains to be seen whether the EU will be willing to step

back and look at all personal data flows with the US from a broader perspective than that found in the [*Schrems*](#) decision.

©1994-2025 Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C. All Rights Reserved.

National Law Review, Volume VI, Number 29

Source URL: <https://natlawreview.com/article/tying-it-all-together-safe-harbor-and-security-related-data-flows>