Proskauer

U.S.-EU Safe Harbor Invalidated: What Now?

October 13, 2015

Last week, the European Court of Justice (CJEU) invalidated the U.S.-EU Safe Harbor framework, effective immediately. This momentous decision jeopardizes the continued flow of data from Europe to the U.S. As the Safe Harbor framework has been in place for 15 years and counts more than 4500 companies among its participants, Last week's ruling is poised to have a major impact on U.S.-EU trade, and leaves many businesses wondering if there are any alternatives that will allow them to continue transferring data across the Atlantic without running afoul of the law. Below, we break down the decision and its implications.

What is Safe Harbor?

The European Union Data Protection Directive forbids the transfer of personal data to a country outside the European Economic Area (EEA) unless that country has adequate data protection measures in place. While a number of non-EEA counties – such as Argentina, Canada, Israel, and Switzerland – have been deemed to provide adequate data protection, American data protection laws remain inadequate in the eyes of EU decision makers. This means that those who wish to transfer personal data from the EEA to the U.S. have to jump through a few more hoops to ensure that the transfer is legal under the Directive. Naturally, this situation is less than ideal, given the volume of trade between the U.S. and Europe.

Enter the Safe Harbor framework, which was designed to facilitate data transfers between the EEA and the U.S. American companies could self-certify that they complied with the Safe Harbor framework, which essentially amounted to their public attestation that they complied with certain European privacy standards. Once a company self-certified and became part of the Safe Harbor program, the company could legally receive exports of personal data from the EEA to the U.S. The Safe Harbor program thus provided American companies a relatively headache-free way to comply with European privacy laws and maintain the all-important flow of personal data from much of Europe to the U.S, and many U.S. companies relied on it to carry out data transfers.

How did this decision come about?

American data protection laws have been under increased European scrutiny ever since Edward Snowden revealed the extent and scope of U.S. surveillance around the world. However, the CJEU rendered this decision as part of what's become known as the "Max Schrems" case. Schrems, an Austrian citizen, privacy activist and Facebook user, filed a complaint with the Irish Data Protection Commissioner, asking the Commissioner to prohibit Facebook from transferring his personal data to the U.S. According to Schrems, Snowden's revelations demonstrated that the U.S. did not adequately protect personal data from NSA surveillance activities. The Commissioner refused to investigate the complaint, reasoning that European Commission Decision 2000/520 – which set out the Safe Harbor Privacy Principles – indicated that the U.S. provided adequate privacy protection. Schrems then challenged the decision before Ireland's High Court. The High Court noted that several U.S. federal agencies carried out widespread surveillance of personal data in a manner contrary to Irish privacy laws, and recognized that Schrems effectively was challenging the legality of Decision 2000/520 and the Safe Harbor framework. The High Court then stayed the case while asking the CJEU to determine whether the Commissioner could investigate a claim that a particular country's data protection laws were inadequate when presented with evidence supporting that theory, even if there already was a decision (such as Decision 2000/520) holding that that country's data protection laws were adequate. In today's decision, the CJEU answered that question in the affirmative, holding that:

the national supervisory authorities, when hearing a claim lodged by a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him, must be able to examine, with complete independence, whether the transfer of that data complies with the requirements laid down by the [EU Data Protection] [D]irective.

See ¶ 57. The CJEU clarified that although the Commissioner could investigate Schrems' claim, neither the Commissioner nor the High Court could invalidate a Commission decision; only the CJEU could take that action.

The CJEU went on to analyze Decision 2000/520 and held that it was invalid. The CJEU found that the Safe Harbor program did not adequately protect personal data from "interference" from the U.S. government "founded on national security and public interest requirements." See ¶ 87. Since EU law only permits such access to personal data where "strictly necessary," and the court described U.S. law as allowing for access to personal data on a more generalized basis, the CJEU found that Decision 2000/520 failed to comply with the Directive's requirements and therefore was invalid.

What's the potential impact of this decision?

The potential impact is significant, given the number of businesses that use the Safe Harbor framework to legally transfer Europeans' personal data to the U.S. It's not just major tech companies that need to make regular transatlantic data transfers: For example, companies that have employees in Europe likely need to transfer those employees' personal data to the U.S. for human resources purposes. Likewise, companies that collect personal data from their European customers may need to evaluate their needs in light of today's decision.

How can companies continue to transfer data in the absence of Safe Harbor?

Despite the alarm surrounding this decision, there are other ways for U.S. companies to transfer data in compliance with European privacy laws. Though more onerous than self-certifying under Safe Harbor, both binding corporate rules and model contracts may be used to effectuate legal data transfers. In addition, the Data Protection Directive allows a data transfer if the data subject unambiguously consents to the transfer, although this option is not favored by some EU data protection authorities and has limited application.

However, it is important to note that the feasibility of these alternative data export options will differ from company to company based on a number of factors. Model contracts, for example, only serve as a practical solution for those transactions where a company, as opposed to an individual, is exporting data to the U.S. If importing data from individual data subjects, companies should ascertain whether these individuals are employees or customers, as it is more difficult to obtain unambiguous consent for transfer from employees than from customers, thereby making that option less appealing for those companies importing employee data. In addition to evaluating their own practices, companies need to reassess their relationships with third-party vendors to whom they have transferred personal information subject to one or both parties' participation in the Safe Harbor program.

Many of the smaller companies that relied on Safe Harbor, though, may not have the resources to take advantage of options other than Safe Harbor. Fortunately for them, U.S. and EU authorities are working together to develop a new Safe Harbor agreement, although it is unclear when this agreement may be finalized.

The true effects of today's decision still remain to be seen, and will play out over the coming weeks and months.

Related Professionals

- **Jeffrey D. Neuburger**
- **Laura E. Goldsmith**
  Partner