Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

The US-EU Safe Harbor Program: Is It Safe?

Law360, New York (May 05, 2015, 10:21 AM ET) --

Devika Kornbacher

Following the revelations by Edward Snowden regarding the U.S. government's mass surveillance programs, European Union lawmakers and data privacy advocates have stepped up efforts to increase data protection measures for EU citizens. One program that became an immediate target for attack was the U.S.-EU Safe Harbor Program. EU law allows companies to transfer EU citizens' personal data outside of the EU only to countries deemed to have an "adequate" level of privacy protection. Because the EU does not feel that U.S. privacy protection laws are "adequate," the Safe Harbor permits companies to transfer EU citizen data to the United States only if those companies voluntarily certify that they comply with certain data protection standards.

With more than 5,000 current registrants, the Safe Harbor is hugely important to companies on both sides of the Atlantic. But the program is in jeopardy, and companies should consider measures to protect themselves in the event the Safe Harbor is suspended.

An Overview of the Safe Harbor

Article 25 of EU Directive 95/46/EC — also known as the EU Directive on Data Protection — requires that EU member states prohibit the transfer of personal data to any country outside the EU that does not "ensure an adequate level of protection." To date, the European Commission, the EU's executive body, has recognized that the laws of only 11 countries or self-governing territories provide adequate protection for EU citizen data. Notably, the United States is not on this list.

In January 1999, the Working Party established by the directive issued its opinion that the "complex fabric of sectoral regulation, at both federal and state level, combined with industry self-regulation" found in the U.S. does not provide adequate protection for EU citizen data. By this point, however, the EC was already talking to the U.S. Department of Commerce about how to allow EU data to be transferred to its biggest trading partner.

In July 2000, the EC approved the Safe Harbor to allow companies to transfer EU citizens' data to the U.S. through a voluntary self-certification program. In the U.S., the Safe Harbor is administered by the Department of Commerce and a company that wishes to join the program must certify annually with the

agency that it will abide by the Safe Harbor's data protection requirements. When a company self-certifies, it commits to a host of requirements falling under seven principles: notice, choice, onward transfer, access, security, data integrity, and enforcement.[1] Depending on the industry sector, the Federal Trade Commission or the U.S. Department of Transportationhandles enforcement against companies that fail to live up to those promises.

Questions About Whether the Safe Harbor Is Actually Safe

The Snowden revelations included details about the NSA's PRISM program, which collects Internet communications of foreign nationals from major U.S. companies, some of which self-certified under the Safe Harbor. These revelations have led many in the EU to question whether the Safe Harbor really offers "adequate" protection for EU data. Germany's data protection commissioners, for example, sent Chancellor Angela Merkel a letter asking her to recommend suspension of the Safe Harbor. And in March 2014, after a six-month investigation into U.S. surveillance programs, the EU Parliament overwhelmingly passed a resolution calling for the "immediate suspension" of the Safe Harbor by the EC and also calling on the U.S. to propose a new framework that would meet EU data protection standards. The EC has acknowledged that the program contains gaps but has nevertheless defended the Safe Harbor as a critical program, both in the court of public opinion and in courts of law.

On March 24, 2015, the European Court of Justice, the EU's highest court, heard arguments in a case that may result in a major threat to the Safe Harbor. The plaintiff, Max Schrems, an Austrian law student and data privacy activist, claims that the Safe Harbor fails to guarantee "adequate" protection of EU citizen data in light of the NSA's activities. Shrems initially challenged Facebook Inc.'s compliance with EU data privacy laws in Ireland, the location of the company's EU base. But the Irish data protection authority rejected his challenge, citing the Safe Harbor. Schrems then appealed to Ireland's highest court, which referred the case to the ECJ. The ECJ is considering whether the Irish data protection authority (1) is bound by and may rely on the EC's official decision that the Safe Harbor program provides "adequate" protection for data, or (2) may or must conduct an independent investigation of factual developments since the EC's Safe Harbor decision in 2000 in order to determine whether the Safe Harbor remains "adequate."

Belgium, Poland and Austria agreed with Schrems and joined his case, while Ireland and the EC argued in support of the Safe Harbor. Reports from the hearing suggest that the ECJ judges showed skepticism toward the Safe Harbor. Schrems was apparently so pleased with a line of questioning that he tweeted from the court: "I want to marry the judge." It is not difficult to understand why the judges may have doubted the adequacy of the Safe Harbor, given some of the EC lawyer's statements. At one point, the EC lawyer told a judge, "You might consider closing your Facebook account, if you have one" — essentially admitting that data at a Safe Harbor-certified company is not adequately protected.

Schrems also pointed to the EC's efforts to shore up the Safe Harbor after the Snowden revelations as further evidence that the program fails to provide "adequate" protection. In November 2013, the EC published a set of 13 recommendations aimed at reinforcing the Safe Harbor, in response to "deep concerns about revelations of large-scale U.S. intelligence collection programmes." These recommendations fall under four categories relating to transparency, redress, enforcement, and access by U.S. authorities.[2] The recommendations include requiring self-certified companies to publish privacy conditions of any contracts they enter into with subcontractors (e.g., cloud computing services), requiring the Department of Commerce to monitor systematically the access to information and follow-up given to complaints received by alternative dispute resolution providers, and subjecting companies to ex officio investigations of effective compliance of their privacy policies. The final recommendation

appears directed at the surveillance programs themselves: “It is important that the national security exception foreseen by the Safe Harbour Decision is used only to an extent that is strictly necessary or proportionate.”

Negotiations between the EU and the Department of Commerce regarding implementation of these recommendations remain ongoing more than 16 months since first proposed. In November 2014, U.S. Federal Trade Commissioner Julie Brill said that only 11 of the 13 recommendations could be addressed by either the Department of Commerce or the FTC, and that the two recommendations on access to data by U.S. authorities are outside their jurisdiction. Recently, in mid-March, a delegation of EU members of Parliament visited Washington, D.C., to continue these negotiations. But nothing has yet been finalized, and there is no timetable for an agreement. Schrems’ team cited these protracted negotiations and missing timetable as proof that efforts to fix the admitted flaws in the Safe Harbor were failing.

In defense of the Safe Harbor, Ireland and the EC argued that the program is necessary both politically and economically, and that negotiations with the U.S. are ongoing. They asked the court to let the EC work toward improving the Safe Harbor without inflicting the damage that would result from its suspension.

The ECJ’s advocate general should publish a nonbinding opinion by June 24 of this year, and the court should issue a final verdict by October.

What Changes to the Safe Harbor Might Mean

The EC appears to remain firmly in support of the Safe Harbor, so the greatest threat to the program at the moment is likely from European courts or the national data protection agencies. Schrems’ ECJ case against Facebook involves limited questions from Ireland’s high court about the authority of the data protection agencies. The Irish high court did not ask the ECJ to rule outright whether, in view of the NSA’s activities, the Safe Harbor complies with EU laws.

Thus, the ECJ could limit its decision to the referred questions and not directly address the validity of the Safe Harbor itself. Instead, it might give data protection agencies the authority to investigate the adequacy of the Safe Harbor and make their own decisions regarding whether self-certifying U.S. companies are in compliance with the directive. A number of EU countries whose data protection agencies have already made their positions clear could then find that the Safe Harbor does not provide “adequate” protection and potentially prosecute U.S. companies that have relied on the program for years.

On the other hand, there is the possibility that the ECJ could sua sponte rule that the Safe Harbor fails to satisfy EU laws and order the program’s suspension, as Schrems attempted to argue. Relying on the ECJ’s April 2014 ruling invalidating the EU Data Retention Directive — which required telecom companies to retain mass quantities of metadata for law enforcement — as being contrary to the EU’s Charter of Fundamental Rights, Schrems argued that this precedent required the invalidation of the Safe Harbor in light of U.S. surveillance.

In the face of uncertainty surrounding the Safe Harbor, it is essential that companies formulate strategies to deal with a potential suspension of the program. Twitter Inc., for example, stated in a recent U.S. Securities and Exchange Commission filing that elimination of the Safe Harbor would disrupt its business by requiring duplicative operations in Europe or by limiting its ability to use EU data.

And Apple Inc. recently announced it will spend nearly $2 billion to build two datacenters in Ireland and Denmark, which are expected to come online in 2017.

A suspension of the Safe Harbor would not necessarily mean the end of data transfers from the EU to the U.S., however. Under Article 26(2) and (4) of the directive, the EU provides other avenues companies may take in order to transfer data from the EU to countries without "adequate" data protection laws. While these avenues may not have the flexibility offered by the Safe Harbor, companies should consider whether they could be viable alternatives to the Safe Harbor based on business needs. The first option is model contracts. The EC has issued standardized contractual clauses pertaining to data transfers that require the contracting parties to comply with certain data protection rules. Inclusion of these clauses in contracts creates a form of private safe harbor. However, because the model contracts are written for only two contracting parties, their usefulness in business settings for data transfers involving multiple parties, such as transfer to a U.S. company that outsources some data processing activities to a service provider, may be limited. Another option is the adoption of binding corporate rules, which are internal corporate rules concerning data protection and privacy that, if approved by affected EU Member States, will allow multinationals to transmit data anywhere within the group of entities covered by the rules, even to countries that do not offer "adequate" protection.

Given the uncertainty of the future of the Safe Harbor, companies that currently transfer EU citizen data to the U.S. should give serious thought to the risk of life without the Safe Harbor. It would almost certainly involve more expense and disruption to business. Planning ahead and investigating alternatives is the best way to minimize both.

—By Devika Kornbacher and Jeffrey Han, Vinson & Elkins LLP

Devika Kornbacher is a partner in Vinson & Elkins' Houston office. Jeffrey Han is an associate in the firm's Austin, Texas, office.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] See U.S.-EU Safe Harbor Overview, Export.gov, http://www.export.gov/safeharbor/eu/eg_main_018476.asp.

[2] See Restoring Trust in EU-US Data Flows, European Commission, http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm.

All Content © 2003-2015, Portfolio Media, Inc.