LOS ANGELES
Daily Journal
www.dailyjournal.com
MONDAY, JANUARY 25, 2016

New safe harbor is a priority for the EU

By Richard Neff

In October 2015, the European Court of Justice issued a ruling that invalidated the safe harbor program for the transfer of personal data from the European Union to the United States. The case involved a 20-year-old EU directive stating that personal data only may be transferred to countries outside the EU which guarantee an adequate level of protection.

Initially, the U.S. was deemed by the EU not to guarantee such level of protection. In 2000, however, the U.S. and the EU agreed on a Safe Harbor Framework, administered by the U.S. Department of Commerce, under which participating U.S. companies would self-certify that they give adequate protection to the personal data of Europeans (basically in accordance with European laws), which has governed such transatlantic data flows for 15 years. Over 4,000 U.S. companies had certified their compliance as of the date of the invalidating legal decision.

On Jan. 7, the European data protection supervisor published his priorities for 2016, indicating that a priority in light of the invalidation of the safe harbor program is a new legal framework with the U.S. for cross-border data flows.

The case last year arose from a complaint by an Austrian student, Max Schrems, regarding Facebook's processing of his personal data from its Irish subsidiary to its servers in the U.S. Schrems was studying at Santa Clara University School of Law, and learned from Silicon Valley tech executives who addressed his privacy class that they did not take European privacy laws very seriously. This led to an idea for a paper topic — to see how Facebook dealt with is privacy data.

Under European laws, European nationals have the right to see all of the data a company has collected about them. After intense email communication with Facebook, he was sent a CD with over 1,200 pages of information about him, containing every poke, friend request, etc., including much information he had deleted, which is illegal under European privacy laws. Schrems filed 22 complaints about Facebook's data retention practices and other privacy practices with the Irish data protection commissioner (Facebook's European operations are based there). Had Facebook been less cavalier with his data, it seems, the case would not have arisen.

Schrems complained that "in light of the revelations made in 2013 by Edward Snowden concerning the activities of the United States intelligence services (in particular the National Security Agency), the law and practice of the United States do not offer sufficient protection against surveillance by the public authorities." The European Court of Justice held the safe harbor principles to be invalid because they do not require all organizations which could work with EU privacy-related data to comply with the principles. U.S. agencies were not required to opt in to use the data, so privacy guarantees under the safe harbor program were insufficient.

It is ironic that the ECJ decision came just over a month before the horrific ISIS attacks on innocent civilians in Paris, leading to much soul-searching in Europe about agency coordination against terrorism. If anything, this event could help accelerate a reasonable new agreement between the EU and the U.S. on cross-border data flows, as European privacy concerns may for the moment play second fiddle to the need for enhanced data sharing so that law enforcement on both sides of the Atlantic can act against the growing terror threat outside the Mideast.

Within one month of the ECJ decision, the EU struck a new data-sharing deal in principle with the U.S. to allow personal digital information to flow between the two economic blocs. The new safe harbor principles would require greater oversight from the U.S. Commerce Department and the Federal Trade Commission. The system will no longer be purely self-regulating, requiring proactive oversight by the federal government as well as significant enforcement, including sanctions. Consumers would be given mechanisms to seek redress for personal data misuse. A European annual review would investigate whether the U.S. government was adhering to limits placed on access to Europeans' data, one of the more controversial points in the agreement in principle.

Schrems complained that 'in light of the revelations made in 2013 by Edward Snowden concerning the activities of the United States intelligence services (in particular the National Security Agency), the law and practice of the United States do not offer sufficient protection against surveillance by the public authorities.'

The European data protection supervisor's priorities published earlier this month stated that he will provide comments on the European Commission's upcoming decision for a new arrangement for the transfer of personal data to the U.S. He also will provide comments on the European Commission's decision regarding the powers of local data protection authorities with respect to existing adequacy decisions.

The goal is to have a new safe harbor framework in place in early 2016. European privacy regulators set a deadline for the end of this month for the new agreement, and have stated that they will not bring widespread coordinated enforcement actions until this "grace period" expires at the end of January, although they will continue to investigate specific cases based on individual complaints.

What now? For the time being, the Department of Commerce has posted the following on its export.gov website: "In the current rapidly changing environment, the Department of Commerce will continue to administer the Safe Harbor program, including processing submissions for self-certification to the Safe Harbor Framework." Companies that have considered compliance with the existing Safe Harbor Framework and need to receive personal data from European countries (e.g., HR data from their European subsidiary, or European customer data), should not hesitate to take advantage of the department's continued administration of the invalidated program. The new framework likely will include most of the existing framework, plus some additional requirements, most of which may fall on the federal government. The framework requirements, and what it means to be in essential compliance with European personal data/privacy requirements, can be found on the department's website.

For most companies which self-certified under the invalidated framework, the next few months (until an agreement is reached) will be a period of great uncertainty in transatlantic personal data transfers. It is likely that such companies can continue to do business as usual, in the expectation that enforcement is unlikely to be very active during a period of regulatory flux.

However, I would advise high-profile transnationals such as Amazon and Google, and especially Facebook, to proceed with great caution, and do everything in their power to be purer than Caesar's wife with respect to European data protection requirements and data flows, until there is greater certainty. The spotlight will surely continue to focus upon their actions.

Richard Neff *is an international IP and privacy lawyer based in Southern California. You can reach him at (310) 321-7660 or richard@nefflaw.com.*

RICHARD NEFF
IP and privacy lawyer