Privacy Alert: EU-U.S. Safe Harbor for Data Transfer No Longer Valid

October 8, 2015

By Michael Cohen (CIPP/US, CIPP/E)

On October 6, the European Court of Justice ruled that the 15-year-old Safe Harbor framework used by thousands of American businesses to transfer personal data from the 28 member countries of the European Union to the United States was immediately invalid.

What was the Safe Harbor?

In Europe, privacy has long been considered a fundamental human right. The collection, use, and transfer of personal information are specifically governed by the EU Data Protection Directive which is in the process of becoming a General Data Protection Regulation.

According to the Directive, personal data cannot be transferred to any country outside the EU that is considered to have inadequate data privacy protection. The United States is one of those countries. As a result, transfers of personal information from the EU to the United States are prohibited unless the business 1) uses EU-approved binding corporate rules (BCR's), 2) uses EU-approved model contract clauses, or 3) (until now) complies with the EU-U.S. Safe Harbor framework.

In 2000, to accommodate EU privacy concerns and allow for the transfer of personal data from the EU to the United States, the United States Department of Commerce reached agreement with the European Commission on certain Safe Harbor privacy principles and a process allowing a business to self-certify to the process and privacy principles. Over 4000 companies have participated in the Safe Harbor framework.

In the wake of revelations by Edward Snowden about US government surveillance and the perceived lax enforcement by the FTC of Safe Harbor compliance, European regulators have publicly questioned the efficacy of the Safe Harbor program. The FTC has responded with a number of enforcement actions, and for the past two years, the United States and the EU have been working on a new Safe Harbor agreement.

For more information on the Safe Harbor framework and alternative compliance methods, see pages 111-116 of A Legal Guide to Privacy and Data Security.

What is the potential impact of the October 6 ruling?

The EU-U.S. Safe Harbor framework is invalid **immediately.** A business can no longer depend upon the Safe Harbor as a defense against claims it violates European data privacy laws. Many were surprised that the European Court did not provide for some reasonable period of time to allow businesses to prepare for this draconian end to Safe Harbor**.**

A data protection authority (DPA) in the EU is now authorized to examine complaints brought to them by data subjects and to pursue investigative actions as necessary to determine if the transfer of personal data is proper under the relevant data protection laws. Data flows could be suspended and fines imposed. We are likely to see a wave of complaints that trigger investigations and enforcement actions against American companies.

If you are a business that has depended upon safe harbor protection or is otherwise involved in the movement of personal data between the European Union and the United States, don't panic.

While the decision takes immediate effect, it is unlikely that the DPA of any particular country will promptly initiate any investigations or challenge the data privacy practices of an American business. It may take some time for each DPA to figure out exactly what they can and should do as result of this decision.

It is also important to note that this ruling does not give the DPA authority to pursue any business directly, but only to investigate the allegations made by a data subject through a formal complaint. We will all anxiously observe the consequences of this decision as it percolates through the regulatory and enforcement process.

However, a business should not wait for a complaint to surface. Now is the right time to consider the data flows relative to personal information from the EU, and what risks exist with any particular country and DPA. If you depended upon Safe Harbor, explore the alternative methods for compliance such as EU approved BCR's, model contract clauses, consent, and other options based upon your unique circumstances. Some large technology companies are already considering EU based cloud providers or otherwise making sure that personal data never leaves the EU—not even a transfer to a server in the United States. The loss of Safe Harbor should result in a search for new ways to assure compliance with European privacy laws.

How did this happen?

In 2013 Max Schrems filed a complaint with the Irish DPA claiming that United States law and practices gave inadequate protection to personal information of EU citizens. Schrem's complaint was based on his use of Facebook and their transfer of his personal information to a server in the United States. He alleged that the Snowden revelations and possible government access to his personal information held by Facebook was a violation of EU privacy law. The Irish DPA rejected his complaint, determined that Facebook was

covered by the Safe Harbor, and was not required to investigate the matter any further.

Schrems then went to the Irish High Court, which referred the case to the European Court. The EU Advocate General, who serves as an advisor to the European Court, issued an opinion that that went much further than expected. The Advocate General's opinion covered not just the rights of a DPA to investigate complaints related to adequacy of privacy protection. It also challenged the validity of the entire Safe Harbor framework. For the most part, the October 6 European Court decision followed the opinion of the Advocate General and declared the entire Safe Harbor framework invalid.

The United States government has been aggressively lobbying to maintain the Safe Harbor and working with EU officials to keep it going. Thousands of businesses rely upon Safe Harbor for the movement of information. The Advocate General's opinion and the European Court ruling went far beyond the narrow questions raised by the Irish High Court. The European Court could have simply referred the case back to the Irish High Court with a ruling that a DPA is permitted to further examine Schrems's complaint. There was no need to also declare the Safe Harbor invalid. This decision of the European Court clearly demonstrates EU dissatisfaction with the United States approach to privacy and a concern with the Snowden revelations.

The good news is that we can help you evaluate the other options that may be available to comply with European privacy law. If you have any questions about the impact of this ruling, please contact Michael Cohen at michael.cohen@lathropgpm.com (612.632.3345).