Solving the Effects of the European Union's Invalidation of the Safe Harbor for International Data Transfers

By Serene K. Zeni / Nov 10, 2015

On October 6, 2015, the Court of Justice of the European Union (CJEU) completely disrupted the international data sharing standards in a pivotal case. In *Maximillian Schrems v Data Protection Commissioner,* Case C-362/14, Mr. Schrems appealed a decision by the European Union's (EU) Data Protection Commissioner not to investigate his complaint regarding the transfer of his personal data from Facebook Ireland Ltd ("Facebook Ireland") to the United States (US) where the data is kept on servers. The decision has US companies scrambling to find alternatives in light of the decision with an approaching deadline of January 31, 2016 having been established by European data protection agencies. The urgency to understand the scope, effect, and alternatives for international data transfers cannot be understated.

Underlying the genesis of the "Safe Harbor" relied upon by more than 4,400 US and European companies regularly participating in data exchange with Europe is Europe's skepticism with the ability of US companies to provide adequate data protection in comparison to the EU's high standards. As of October 1998, the European Commission's Directive on Data Protection ("Directive") prohibits the transfer of data to non-EU countries that do not meet the EU's "adequacy" standard for privacy protection. Because of the stark difference between the US and EU in data privacy protection, the US Department of Commerce in consultation with the European Commission developed a "Safe Harbor" in 2000 which, if met, would allow US and European companies to be deemed "adequate" without having to comply precisely with the Directive. Organizations that decide to participate in the "Safe Harbor" program must comply with certain standards, in addition to the organization's home country standards, pertaining to notice to consumers, the choice to opt out of data sharing, disclosure regarding transfer of information to third parties, access to consumers of their own information, reasonable data security precautions to prevent misuse, ensuring data integrity, and mechanisms to enforce compliance.

The "Safe Harbor" has primarily been enforced in the US under US law and is largely dependent on private sector self-regulation backed by government enforcement of federal and state unfair and deceptive practices statutes. An organization could self-certify as compliant with the "Safe Harbor" and, thus, experiences little government oversight. In fact, Edward Snowden's leak of classified information in 2013 revealed the weakness of such self-regulation and the consequential government benefit. The Snowden revelations showed United States intelligence agencies had large-scale access to data exchange, whether or not international. As such, the CJEU concluded reliance on entities to self-certify compliance resulted in looser data protection which, in effect, allowed US intelligence agencies to tap into commercial internet service providers more freely.

The purpose of the "Safe Harbor" was to streamline data communication and make data sharing for companies like Facebook and Google cost-effective. However, the "Safe Harbor" did not only benefit traditional "tech" companies. Any company with offices in the EU transferring personal data to the US is subject to the Directive and, therefore, benefits from the "Safe Harbor." Because enforcement was largely based on self-regulation, companies were able to self-certify they had appropriate privacy measures in place. Without the "Safe Harbor," US companies participating in data transfers with the EU face greater regulation because the EU's position on personal data protection is that it is a fundamental right, which is not the case in the US. Thus, US companies will have to comply with the EU's high threshold for personal data protection, will encounter more layers of oversight as both governments will enforce their standard regulations, and, as a result, experience increased cost to comply. EU companies are not affected by the decision unless they have offices in the US accepting data transfers from the EU because data transferred from the US to the EU is not subject to the Directive.

In Mr. Schrems' appeal, he argued enabling the transfer of his data between the US and EU under the less stringent requirements of the "Safe Harbor" is a violation of his fundamental right to privacy protected under the European Convention for the Protection of Human Rights and Fundamental Freedoms. The CJEU agreed and ruled the "Safe Harbor" framework gave the American government routine access to the information of Europeans and is, therefore, counter to their fundamental right to privacy.

Practically, the effects of the ruling may be tempered or avoided. The ruling does not immediately require the restoration of data to its place of origin as may be the case with Mr. Schrems if Facebook Ireland cannot comply without the Safe Harbor through other means discussed below. It simply allows each EU member state to rule for its own citizens whether the agreement is illegal. It is very unlikely, however, a national court will rule contrary to the CJEU, which is interpreting the same laws that would be at issue in a national case.

International organizations in particular industries such as health care, which are already overwhelmed with higher burdens regarding data protection, as well as those not large enough to partake in alternate avenues for protection, may struggle without another safe harbor agreement in place to remedy the consequences of this decision. Currently, US leaders are working to negotiate another agreement in the wake of the CJEU ruling. On October 26, 2015, the EU announced it had reached a tentative agreement "in principle" with the United States on a new data-sharing plan. However, European data protection agencies have only given the US and EU until January 31, 2016 to enter into a new agreement, threatening to take action against US companies transferring data from the EU if no formal agreement is reached by then. Without stricter data security rules, however, it is unlikely another agreement will overcome future scrutiny. On November 3, 2015, the United States Congress began holding public hearings on digital trade trying to determine how to balance the interests of the government in accessing information, companies in the free flow of information, and individuals in their right to privacy protection. On November 6, 2015, European officials indicated they expect to complete a new trans-Atlantic data sharing agreement in the next three months.

While the respective governments scramble to solve the impact of the CJEU decision, the following actions can be taken by a company to avoid its

reliance on a governmental resolution:

Informed Consent. The EU Directive allows for transfer where the "data subject has given [his or her] consent unambiguously to the proposed transfer." Although informed consent is an option, the threshold for obtaining informed consent is arguably high and dependent on the relationship of the parties and other contextual factors.

"Standard Contractual Clauses." As another alternative, back-up agreements may be in-place or put in-place to protect against liability without the "Safe Harbor." "Standard contractual clauses" adopted by the European Commission can be integrated into these agreements between US and European organizations exchanging data to ensure US organizations make certain commitments with respect to the handling of data.

Corporate Governance. A company can adopt internal rules, protocols, and procedures to define its global policy with regard to international transfers of personal data within the same corporate group to entities located in countries that do not provide an adequate level of protection.

Corporate Assessment. A company should analyze its data protection standards to determine where it stands without "Safe Harbor" protection. For example, a company should look at its data flows, assess scale and sensitivity of the information being shared, and look at existing contracts with cloud-based vendors.

The undertaking to minimize the impact of the CJEU ruling is great and must occur rapidly before its effects are felt. The US government will surely face a long road in trying to balance the interests of all stakeholders as it develops legislation and seeks a new safe harbor agreement with the EU. Because of the impending deadline and ongoing efforts to resolve the issues, it is important to keep up with new developments in crafting solutions. Companies must not delay in taking action to safeguard their interests and prevent impediments to international data transfers.