Uncharted Waters: Navigating Data Transfers After Safe Harbor

By Alan Seem, Richard Hsu and Mark Langer

The past six months have seen sweeping changes to the global privacy landscape spearheaded by the European Union (the “EU”). In October 2015, the Court of Justice for the European Union (the “CJEU”) shocked the privacy world by striking down the Safe Harbor Privacy Principles framework (the “Safe Harbor”), the backbone of international data transfers between the EU and the United States, exposing thousands of companies to the risk of enforcement actions. Then, in December 2015, the EU concluded almost four years of negotiations regarding its new General Data Protection Regulation, which seeks to reform the EU’s current privacy laws and increase the privacy protections of EU citizens and provides for potentially massive fines for non-compliance. While the full impact of these events is still being determined, they clearly represent fundamental changes in privacy practices and data protection worldwide, and it is important for U.S. companies to understand and prepare for them. This article will focus on the end of the Safe Harbor and the pending EU-U.S. Privacy Shield (the “Privacy Shield”) that is meant to serve as its replacement.

The Origins of the Safe Harbor Framework

In 1995, the EU’s Data Protection Directive 95/46/EC (the “Data Protection Directive”) drove a wedge between U.S. and EU privacy regimes, leaving U.S. companies without an efficient method to engage in international data transfers. The Safe Harbor was initially created to bridge that divide. The Data Protection Directive provided a comprehensive guide for the privacy regulations of its member states, and it included a requirement that the personal data1 of EU residents could only be transferred to countries that guaranteed adequate protection2 of that personal data.

1 Under this directive, “personal data” is defined as any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

2 The Data Protection Directive requires that there are adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and regarding the exercise of the corresponding rights.
information. This created a significant obstacle for U.S. companies, as the United States does not have one comprehensive privacy law governing all industries, but rather a patchwork of sectoral regulations administered by different government agencies. Without a comprehensive privacy law in place, the U.S. was deemed at that time to be a jurisdiction that did not provide adequate protection, effectively blocking the transfer of the personal data from the EU.

In 2000, after years of discussions between representatives of the EU and the U.S., the Safe Harbor was proposed. Under this framework, U.S. companies were required to adhere to seven privacy principles (which relate to notice, choice, onward transfers, access, security, data integrity and enforcement) in their collection and management of personal data. The framework utilized a self-certification model administered by the U.S. Department of Commerce. In July 2000, the European Commission formally adopted the Safe Harbor, declaring that any U.S. company that adhered to the framework would have the adequate privacy protections necessary for international data transfers.

The Safe Harbor provided an efficient solution for businesses, but it drew criticism from some privacy advocates, who argued that it did not do enough to protect individuals’ privacy. Despite the complaints, the number of corporate participants in the Safe Harbor grew exponentially over the next fifteen years, with over four thousand companies self-certifying. With so many companies certified and so much data being transferred, no objection seemed strong enough to challenge the Safe Harbor.

The Demise of the Safe Harbor: Schrems v. Data Protection Commissioner

In 2013, in response to the Edward Snowden revelations about U.S. government surveillance, an Austrian student and privacy activist brought a complaint to the Irish data protection commissioner regarding Facebook’s collection and transfer of personal data. The Irish data protection commissioner, citing the European Commission’s validation of the Safe Harbor, stated that it did not have the authority to find that Facebook’s actions violated the Data Protection Directive. The case, and specifically the question of the validity of the Safe Harbor, eventually made its way before the CJEU.

In October 2015, the CJEU invalidated the European Commission’s decision that the Safe Harbor provided adequate protection. To support its holding, the CJEU pointed to a few key flaws with the Safe Harbor. First, the Court noted that the Safe Harbor provided insufficient
protections against the surveillance by U.S. public authorities of transfers of personal data. Second, the Court stated that the Safe Harbor did not provide adequate legal remedies for EU residents with claims that their privacy rights had been violated. The Court also held that the European Commission did not have the power or authority to restrict national data protection authorities from conducting their own investigation regarding whether a foreign jurisdiction’s privacy protections were adequate.

The Privacy Shield

In the wake of the Schrems judgment, lawmakers in the U.S. and Europe started negotiating a new framework, one that would fill the void created by the CJEU’s ruling. Although the CJEU’s decision to invalidate the Safe Harbor became effective immediately, the data protection authorities in the EU suspended any enforcement actions until the end of January, giving lawmakers time to reach an agreement.

On February 2, 2016, U.S. and EU officials announced that a new agreement had been reached, and the full draft of the proposed Privacy Shield was officially released on February 29, 2016. This new framework is still under review by EU data protection authorities and the Article 29 Working Party and has yet to be formally adopted, but companies now are able to see what the future cross-border privacy landscape may entail. While in some ways the Privacy Shield resembles the Safe Harbor, the Privacy Shield creates some new obligations for companies, including:

1. **Certification and Compliance.** Like the Safe Harbor, the Privacy Shield requires self-certification through the U.S. Department of Commerce. Under the new framework, however the Department of Commerce will also be conducting its own *ex-officio* investigations to ensure that companies are complying with the requirements of the Privacy Shield. Companies are required to maintain records of their compliance with the Privacy Shield and to promptly assist with these investigations. The Department of Commerce will also maintain a list of Privacy Shield participants on its website, along with a list of any entities that were once certified but have lost or ended their certification.

2. **Enforcement and Sanctions.** The new Privacy Shield has many potential enforcement agents, among which are the Federal Trade Commission (the “FTC”) and the Department
of Commerce in the U.S., independent dispute resolution bodies in the EU and the U.S., and, in some limited cases, even EU data protection authorities. The FTC will be the leading enforcement agency in the U.S. and has recommitted itself to prioritizing privacy complaints and reviewing referrals from other entities, such as the Department of Commerce and EU data protection authorities. The Privacy Shield also provides for sanctions for non-compliance, including public notice of findings of non-compliance, deletion of data, injunction awards, compensation for individuals, and suspension or removal of the Privacy Shield certification. The public nature of compliance and non-compliance, as seen with the sanctions and the publicly available list of Privacy Shield members, will likely be an important tool for enforcement agencies to demonstrate the Privacy Shield’s effectiveness.

3. **Recourse for Individuals.** Not only does the Privacy Shield provide for enforcement by various agencies, but it also mandates that companies develop robust procedures for addressing individual complaints. The Privacy Shield requires companies to respond to an individual’s complaint within 45 days and provide independent recourse mechanisms to individuals free of charge. Companies also must provide individuals with notice, both of any information collected (as well as access to that information) and the recourse available to individuals under the Privacy Shield.

**Looking Forward**

Even with the support of the European Commission, the Privacy Shield is far from set in stone. Some European data protection authorities have already voiced their concern with the Privacy Shield, and the Article 29 Working Party has not completed its review of the framework. Even if the Privacy Shield is adopted in its current form, it may still be challenged in the CJEU. Furthermore, U.S. companies must decide whether the Privacy Shield is the right option for them, especially as the many agencies tasked with enforcing the Privacy Shield will be scrutinizing early adopters of the Privacy Shield to determine its effectiveness.

In light of the proposed framework and current political uncertainties, below are a few suggestions that companies should consider:

1. **Know where you could be exposed.** Ensure that you have a clear understanding of how your company collects and uses personal data and the life cycle of that data. What
information are you collecting from your customers and partners? What is the country of origin of such data? How is that data maintained and protected? What international data transfers are occurring? Are they necessary or can they be terminated or postponed?

2. Review the terms of the proposed Privacy Shield. Although the Privacy Shield has not yet been formally adopted, companies should familiarize themselves with the requirements of the Privacy Shield and consider whether it would be suitable for them. Even if the Privacy Shield is not ultimately adopted, it outlines some of the key practices that will likely be part of any future framework.

3. Consider existing alternatives to the Privacy Shield. The grace period granted by the EU data protection authorities and Article 29 Working Party has not been extended past January 2016, and companies that are still transferring data under the Safe Harbor are at risk of enforcement actions. The Data Protection Directive provides other methods for managing these types of transfers, including model contract clauses and binding corporate rules. Review these alternatives and consider which might be best for your company. However, bear in mind that these alternatives are not infallible and may, too, be invalidated by the CJEU.

4. Address complaints. Confirm that you have processes in place for addressing individual privacy complaints. This is an important element of the Privacy Shield and will continue to be an important part of providing adequate protections going forward.

5. Monitor enforcement. Monitor privacy enforcement actions in the EU member states from which your company transfers data. These actions, as well as the basis upon which they are brought and the type of companies that are targeted, can serve as a good indication of whether your company may be at risk for similar enforcement actions.

---

3 The European Commission has issued two sets of standard contractual provisions for transfers from data controllers to data controllers established outside the EU and one set for the transfer to data processors established outside the EU.

4 These are internal rules (such as a code of conduct) that may be adopted by a company or a group of companies that define its global policy with regard to the international transfers of personal data within the same corporate group to entities located in countries which do not provide an adequate level of protection (as defined by the Data Protection Directive).