Taking Advantage of Privacy Shield Protections: Part I

Christopher M. Brubaker, The Legal Intelligencer

March 16, 2016

This is the first of two parts providing an overview and analysis of the EU-U.S. Privacy Shield Agreement. The first part focuses on the general framework of the Privacy Shield and on the responsibilities of the private sector in taking advantage of the protections offered by the Privacy Shield: self-certification; review by the U.S. Department of Commerce; the principles (transparency, quick attention to consumer inquiries and complaints, free (to consumer) dispute resolution mechanisms); and cooperation with data protection authorities. Part **II** will look at the primary government responsibilities in terms of enforcement and the U.S. government's agreements to limit bulk data collection and provide analysis of the framework.

On Feb. 29, the U.S. Department of Commerce and European Commission released the full text of the new EU-U.S. Privacy Shield Agreement, the much anticipated replacement for the Safe Harbor framework, to allow transfer of personal information of people living in the European Union to the United States for commercial purposes. The Privacy Shield comes at a critical time as there is increasing uncertainty regarding the legality of data transfers in the wake of the European Court of Justice's (ECJ) Oct. 6, 2015, decision invalidating the Safe Harbor framework. While the Privacy Shield would give U.S. businesses the certainty they desire, as will be discussed below, final acceptance and implementation of the Privacy Shield, at least in its present form, is far from certain. With that caveat, it is important to become familiar with the Privacy Shield as the general framework is likely to be included in substantial form when an agreement is finalized and following its requirements will likely give some protection in the interim.

The basic premise of the Privacy Shield is to ensure that personal data of European nationals that is transferred to the United States for commercial purposes is subject to the same data protection standards that are required in the EU and to provide individuals with the methods to ensure compliance. The Privacy Shield, as proposed, appears to accomplish these objectives with a multilayered process for implementing, monitoring and enforcing the necessary data protection standards. The buzz words being touted in the official release documents include "transparency," "stronger obligations," "robust enforcement and monitoring," and "clear safeguards." The likely sticking point to acceptance and implementation has to do with collection of data by the National Security Agency and other government agencies.

PRIVACY SHIELD OVERVIEW

- **Self-reporting.**

To take advantage of the Privacy Shield, companies will need to register on the Commerce Department's Privacy Shield register and certify compliance with Privacy Shield's requirements (principles) on an annual basis. This includes publishing privacy policies detailing the data safety standards followed by the company as well as explaining the dispute resolution mechanisms afforded by the Privacy Shield and how they can be utilized. Organizations can also elect to

have the Privacy Shield protections apply to human resources data transferred from the EU, but must so state on the self-certification.

- **Review by Commerce Department.**

The Commerce Department is tasked with maintaining two registries, one for self-certifying companies in good standing (i.e., eligible for the Privacy Shield) and one for those entities no longer eligible whether they have voluntarily withdrawn or have been removed for cause. Companies that are removed from the list for noncompliance must return or delete information they have obtained. Companies that voluntarily withdraw and wish to retain data must continue to annually certify that they will continue to maintain the data in adherence to the principles. The Commerce Department has committed to reviewing self-certifications to make sure they contain all required information and independently verifying items such as publication of privacy policies on websites, membership in third-party organizations, and similar items as applicable to the particular certification.

- **Principles.**

The principles consist of seven numbered sections addressing: 1. Notice (covering 13 different aspects of data collection, storage and use); 2. Choice (opt-out procedures regarding disclosure to third parties or for uses different than what the data was originally collected for); 3. Accountability for onward transfer (collecting entity remains liable when utilizing third parties as agents and must oversee agents' adherence to principles); 4. Security (reasonable and appropriate measures to protect data); 5. Data Integrity and Purpose Limitation (use and process consistent with the reason it was collected); 6. Access (individuals must have access to information that is collected); and 7. Recourse, Enforcement and Liability (this is multilayered and will be discussed in more detail below). There are also 16 supplemental principles addressing certain points from the principles in more detail and also noting exceptions to the principles.

- **Recourse, enforcement and liability.**

This is the crux of the Privacy Shield and designed for addressing issues identified with the Safe Harbor framework even before it was invalidated. "Effective privacy protection must include robust mechanisms for assuring compliance with the principles, recourse for individuals who are affected by non-compliance with the principles, and consequences for the organization when the principles are not followed," as in Principles, Section 7(a). This means, at a minimum: (1) free, readily available independent recourse mechanisms to investigate and resolve complaints and disputes including the awarding of damages available under applicable law; (2) procedures to verify that attestations and assertions made about privacy practices are true and have been properly implemented; and (3) sanctions for failure to comply with the principles sufficiently rigorous to ensure compliance. (Subparts (a)(i) and (a)(iii) are further addressed in supplemental principles 5 and 11, and subpart a(ii) in supplemental principle 7.) Companies must respond promptly to requests for information or complaints referred through the Commerce Department and agree to arbitrate claims as set forth in Annex **I.**

- **Cooperation with data protection authorities.**

Companies can satisfy subparts (a)(i) and (a)(iii) by committing to cooperate with EU data collection authorities (DPAs) in their self-certification submission. This requires cooperation with

DPAs in the investigation and resolution of Privacy Shield complaints and complying with any advice given by the DPAs that the organization needs to take specific action to comply with the principles including remedial or compensatory measures for the benefit of the individual. This will be administered through a panel of DPAs established at the EU level to ensure a harmonized and coherent approach. Advice will only be issued after both sides have had a reasonable opportunity to comment and provide any evidence they wish.

- **Address complaints within 45 days.**

Companies are encouraged to create internal grievance procedures to address consumer complaints that can be utilized prior to or in conjunction with other mechanisms. Consumers are to be encouraged to raise complaints directly with the company before exercising their rights under the independent recourse mechanisms. The section on cooperation with DPAs expressly states that DPAs will encourage consumers to avail themselves of such procedures if available and appropriate to the issue raised, before conducting a formal advice procedure. Companies must respond to consumer complaints within 45 days.

- **Alternative dispute resolution.**

Companies not opting to cooperate with DPAs must create and maintain "independent recourse mechanisms" that are readily available and free to consumers. These dispute resolution bodies must look into any complaint that is not obviously frivolous or unfounded and provide readily available information about how the procedure works and cooperate in the implementation of standard tools or processes such as a standard complaint form. Other information that must be provided include links to the applicable principles, the Commerce Department's Privacy Shield website, state that the service is free, how a complaint can be filed, the timeframe for resolution of complaints, and a range of potential remedies. Annual data must also be provided about how the process is actually working. The Privacy Shield also establishes an arbitration procedure for "residual claims" that do not get resolved by any of the other available methods.

Christopher M. Brubaker of Clark Hill concentrates his practice in complex commercial litigation and insurance matters. He regularly provides advice to companies on insurance and cyberrisk issues related to transactions and risk management and also advised companies on regulatory matters involving insurance and environmental laws, rules and regulations. He frequently speaks and writes on cybersecurity matters for legal and professional groups.