Privacy Shield: Gov't Responsibilities, Bulk Data Collection: Part II

Christopher M. Brubaker, The Legal Intelligencer

March 23, 2016

This is the second of a two-part look at the new EU-U.S. Privacy Shield Agreement. The first part looked at the general framework of the Privacy Shield and focused on the responsibilities of the private sector in taking advantage of the protections offered by the Privacy Shield, such as 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 (DPAs). Part II addresses 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.

Enforcement by FTC and DOT

Companies that opt to self-certify are subject to the jurisdiction of the Federal Trade Commission (FTC), the U.S. Department of Transportation (DOT) or other subsequently designated agency. These agencies will be cooperating with DPAs to investigate and resolve complaints raised with the DPAs. The Privacy Shield package contains letters from both the FTC and DOT outlining their commitment to enforcing the Privacy Shield. (The FTC's submission also contains an overview of its current cybersecurity enforcement initiatives and guidelines.) Thus, even if a company does not opt to cooperate with DPAs to satisfy the requirements of subparts (a)(i) and (a)(iii), they are still subject to "cooperate" through the investigatory and enforcement powers of either the FTC or DOT. In addition, the FTC has the authority to enforce failure to comply with the self-reporting requirements as an unfair or deceptive trade practice under 15 U.S.C. Section 45(a).

Limitations on Bulk Data Collection and Ombudsman

The Privacy Shield documents include a letter written by general counsel Robert Litt from the Office of the Director of National Intelligence, summarizing the U.S.'s revised policies governing bulk data collection found in Presidential Policy Directive 28, which only allow bulk data collection for six specific purposes: detecting and countering certain activities of foreign powers; counterterrorism; counterproliferation; cybersecurity;

detecting and countering threats to United States or allied armed forces; and combating transnational criminal threats, including sanctions evasion. The letter also notes that all data collection is subject to constitutional, statutory and oversight protections. Secretary of State John Kerry also provided a letter outlining the creation of an ombudsman, who is independent of the national security services, to oversee and address complaints from individuals related to data transferred under the Privacy Shield and other - applicable methods. In its cover document transmitting the Privacy Shield documents to the European Parliament and Council ("**Communication From the Commission to the European Parliament and the Council—Transatlantic Data Flows: Restoring Trust Through Strong Safeguards")**, the commission summarized the protections afforded to individuals from bulk data collection efforts by U.S. government agencies, stating: "For the first time, the U.S. government, through the Department of Justice and the Office of the Director of National Intelligence as the body overseeing the entire U.S. intelligence community, has provided the EU with written representations and assurances that access by public authorities for law enforcement, national security and other public interest purposes will be subject to clear limitations, safeguards and oversight mechanisms. The U.S. will also establish a new redress mechanism for EU data subjects in the area of national security through an ombudsperson who will be - independent from the national security authorities. The ombudsperson will be tasked with following-up complaints and enquiries by EU individuals into national security access and will have to confirm to the individual that the relevant laws have been complied with or that any non-compliance has been remedied. This is a significant development that will apply not only to Privacy Shield transfers but to all personal data transferred to the U.S. for commercial purposes, irrespective of the basis used to transfer those data."

ANALYSIS

While government officials from both the EU and United States, as well as industry groups such as the Computer & Communications Industry Association, are hailing the Privacy Shield as providing enhanced protection for Europeans whose data is transferred to the United States and certainty for businesses, other commentators are not so certain the Privacy Shield will be formalized as enacted. Indeed, Max Schrems, the Austrian privacy advocate whose challenge to Safe Harbor led to its invalidation, has already spoken out against the Privacy Shield, stating, "Basically, the U.S. openly confirms that it violates EU fundamental rights in at least six cases." A key aspect of the European Court of Justice's opinion invalidating the Safe Harbor framework dealt with

the U.S.'s surveillance methods that were disclosed by Edward Snowden and, in particular, bulk collection of data. "Legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of fundamental right to respect for private life, as guaranteed by Article 7 of the Charter," as in Case C-362/13, *Maximillian Schrems v. Data Protection Commissioner*, EU:C:2015:650, paragraph 94. Other commentators have noted how the EU's Article 29 Working Party, which represents data protection authorities from the 28 member-states, recently published its analysis of the *Schrems* decision, which included four requirements that the new framework should include. In particular, they called for an independent oversight mechanism that is both effective and impartial; either a judge or another independent body, as long as it has sufficient ability to carry out the necessary checks. As the Article 29 Working Party will be tasked with evaluating the Privacy Shield and opining on its compliance with EU standards, it is not clear that the proposed ombudsman procedure will satisfy its desire for an independent decision-maker. Thus, it would seem that the path to finalization and implementation of the Privacy Shield could well be a bumpy one and is far from guaranteed. With that said, the main criticism of the Privacy Shield all seems to be focused on the national security exception and how that will be administered and possibly further limited to comply with EU privacy standards. This would suggest that the remaining aspects of the Privacy Shield will pass scrutiny within the EU and will be part of the final framework. While it is far too early to advise companies to begin to fully implement these procedures, it would be wise to review the principles, to become familiar with the requirements, and to start implementing these practices where feasible as they will likely be legally required sooner than later.

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.