Schnader
ATTORNEYS AT LAW

Schnader Harrison Segal & Lewis LLP

CALIFORNIA DELAWARE JAKARTA* NEW JERSEY NEW YORK PENNSYLVANIA WASHINGTON, D.C.

PRIVACY AND DATA SECURITY AND INTERNATIONAL ALERT

SEPTEMBER 2016

"PRIVACY SHIELD" REPLACING INVALIDATED EU-US SAFE HARBOR AGREEMENT IS OPEN FOR BUSINESS, BUT CHALLENGES TO ITS VALIDITY ARE EXPECTED

By Scott J. Wenner

The Safe Harbor agreement between the European Union and the United States permitted American businesses to import personal data of EU citizens based on self-certification of compliance with EU data protection principles. Safe Harbor was widely criticized in Europe as being too easily circumvented, too infrequently enforced and, in general, offering too little protection to the personal data of EU citizens.

Edward Snowden's 2013 claim that the U.S. National Security Agency ("NSA") was collecting vast quantities of personal data of foreign nationals provided to it by Internet companies dramatically escalated EU criticisms of Safe Harbor. Snowden's revelations led European data processing authorities ("DPAs") and EU representatives to insist on negotiations with the United States to strengthen Safe Harbor if termination of that agreement by the EU was to be avoided.

While negotiations between representatives of the U.S. and the E.U. slowly proceeded, the EU Court of Justice ("ECJ") heard a claim by an Austrian privacy activist, Max Schrems, alleging that Facebook - a Safe Harbor participant - violated the privacy rights of EU citizens that Safe Harbor was supposed to protect by giving their personal data to the NSA. On October 6, 2015 the EUCJ announced its *Schrems* decision, which concluded that the Safe Harbor agreement failed to protect Europeans from unlimited and indiscriminate collection, storage and review of their private information, and thus was invalid. *Schrems* thus swept away the agreement upon which thousands of American companies had predicated their compliance with European national laws enacted to comply with the EU Data Protection Directive (Directive 95/46/EC).

Significantly, the EUCJ also declared in *Schrems* that national DPAs are obliged to challenge European Commission decisions approving agreements such as Safe Harbor, and now the Privacy Shield, when their investigations lead them to believe that such an agreement with a non-EU country fails to protect data privacy rights of their own citizens. With that holding, the EUCJ's ruling removed any legal certainty that Commission approval of privacy agreements negotiated with key trading partners can be relied upon as a final expression of what will be considered lawful before a business implements expensive practices and procedures in reliance to comply with their terms.

Response to Safe Harbor's Demise – The Privacy Shield

The *Schrems* decision caused great concern among the U.S. businesses that were relying on Safe

Harbor for their flow of data from Europe, and created political pressure on the U.S. and EU agencies already negotiating revisions to that agreement. Moreover, the Article 29 Working Party ("Working Party") – an independent and enforcement-oriented advisory body on data protection comprised of representatives of the data protection regulators of all 28 of the member states – had adopted an aggressive posture on the meaning of *Schrems* as applied to the mission of national DPAs. The Working Party declared that the focus of the *Schrems* ruling on the purported overreach of the NSA and complicit businesses at the expense of privacy rights of Europeans would prompt it to reassess the efficacy of all of the tools previously authorized for the transfer of personal data to the U.S. – including standard form contracts between data processors and third parties that it had approved years ago. It ominously added that the DPAs within the EU were prepared to commence "coordinated enforcement actions" and any other "necessary and appropriate actions" against businesses previously reliant on the Safe Harbor if EU and U.S. negotiators failed to reach an appropriate accord by January 31, 2016.

On February 2, EU and U.S. negotiators announced agreement on "a new framework for transatlantic data flows." Dubbed the "Privacy Shield," the agreement was announced long before it ever was committed to writing, such was the urgency to announce a resolution before national DPAs began acting on the Working Party's threat. The information made available by the negotiators consisted only of an outline of broad principles to which EU and United States Commerce Department officials agreed. An EU press release declared only that the Privacy Shield would include:

- "Strong obligations" on U.S. companies on how personal data of Europeans is processed and privacy rights are guaranteed.
- "Robust enforcement," to include monitoring by the Commerce Department of the publication of privacy commitments to allow the FTC to enforce breaches as unfair trade practices.
- Undefined special treatment of human resources data from Europe, which obliquely will require employers to comply with decisions of European DPAs.
- Clear safeguards, limitations and oversight mechanisms applicable to access by public authorities to personal data transferred from Europe to the U.S.
- Effective protection of the privacy rights of EU citizens with eight channels for redress of their complaints and deadlines for their resolution, including free alternative dispute resolution and a referral mechanism from DPAs to the Department of Commerce and the FTC, with binding arbitration for injunctive relief made available as a mechanism of last resort.
- An Ombudsman embedded within the U.S. State Department will be appointed to investigate claims of inappropriate monitoring by U.S. national security agencies.

Given the vital connection the flow of data has to international trade, the lack of certainty in the announcement was unsettling to businesses and regulators alike, as the sketchy announcement did not provide anything concrete to permit planning to go ahead. Meanwhile, the Article 29 Working Party declared that, as the representative of the national DPAs, its approval would be required before the Privacy Shield could move forward, and it gave the negotiators a short and firm deadline by which it expected to receive information necessary for it to conduct the necessary analysis. The Working Party declared that its examination would focus on whether Privacy Shield provided (i) clear, precise and accessible rules for processing personal data; (ii) an appropriate balance between national security objectives and privacy rights; (iii) an independent oversight mechanism to review all surveillance activity; and (iv)an effective remedy for excessive processing activity.

The insistence of the Working Party that its approval would be necessary, the expressions of

doubt among several national DPA representatives who were part of the Working Party and the promises of privacy activists to challenge the Privacy Shield in national forums as well as before the ECJ should its adequacy be approved by the European Commission, all prompted a flurry of activity to respond to the Privacy Shield's critics. Simultaneous with the Commission's release of the details of the agreement in late February 2016, the U.S. Secretary of Commerce released a set of written commitments signed by the heads of U.S. agencies with responsibility to enforce the Privacy Shield. These signed commitments were intended to underscore the U.S. government's intent to meet the concerns that prompted the ECJ to invalidate the Safe Harbor accord, especially the alleged practices of the U.S. intelligence community. Among the written materials released by the American government were letters containing specific representations from the Federal Trade Commission, the Department of Transportation, the International Trade Administration, the Departments of Justice and State, and the Director of National Intelligence. These commitments plainly were intended to meet and neutralize opposition to and suspicion of the Privacy Shield pact from those who characterized it as a warmed over version of Safe Harbor from the outset, and doubted the intention of the U.S. government to enforce it any more rigorously than it enforced Safe Harbor.

Resemblance of Privacy Shield to Safe Harbor

Critics correctly noted that the proposed Privacy Shield was in some respects quite similar to its predecessor. Its resemblance to the Safe Harbor principles is unmistakable, but largely unavoidable; after all, both aim at mandating adherence to the same core set of principles that comprise the EU Data Protection Directive. Thus, much like Safe Harbor, the Privacy Shield is predicated on self-certification by a business to comply with a set of seven privacy principles. These principles include consumer notice; choice; accountability for the consequences of onward transfer; security; data integrity and limitation of the purposes for which the data is used; access; and recourse, enforcement, and liability. It also contains a so-called "supplemental" set of principles that deal with a broad range of issues, including the handling of "sensitive" data (e.g., health, religious, political and similar information), secondary liability of Internet service providers and telecommunications companies, and the role of data protection authorities.

The Privacy Shield's resemblance to the Safe Harbor doesn't end with its principles, however. Like the former program, the Privacy Shield program would be and is administered by the U.S. Department of Commerce, and primary enforcement authority in the United States would reside with the FTC. Like Safe Harbor, the Privacy Shield also is based on self-certification, and businesses are required to re-certify their compliance every year, as they were supposed to do to comply with Safe Harbor. Addressing a major criticism that had been leveled at Safe Harbor, U.S. authorities promised to more diligently monitor the re-certification process under the Privacy Shield - a process that some businesses were found to have ignored with impunity under Safe Harbor.

Addressing ECJ Criticism of Safe Harbor

The Privacy Shield tackles head-on another of the criticisms leveled by the EU Court at the Safe Harbor agreement: redress for violations of the data protection principles. It provides EU citizens with several options for seeking remedies, including via alternative dispute resolution that must be offered free of charge as a condition to signing on to the Privacy Shield. It also allows EU citizens to obtain the assistance of the FTC and/or their national data protection authority ("DPA") to seek redress. The agreement ambitiously requires covered businesses to resolve complaints they receive from EU citizens within 45 days.

The Privacy Shield reserves special attention to the concerns expressed by the EU Court of Justice and the Working Party over the threat to privacy rights of EU citizens posed by American intelligence agency practices, including providing a specific enforcement mechanism for alleged breaches in

the name of national security. The appointment of an ombudsman who would be independent of the intelligence agencies to whom complaints about intelligence oversteps could be directed was promised, and U.S. Under Secretary of State Catherine Novelli was named to this position. In addition, the enforcement mechanism contains limitations on access by national security agencies.

Another new term that was added to strengthen the monitoring and enforcement of compliance is a requirement for a joint annual review of the functioning of the Privacy Shield by U.S. and EU designees, with the participation of national security experts. Each annual review is expected to yield a publicly available report, obviously intended to create transparency to allay the concerns of a dubious European public.

Special Attention to Human Resources Data

While the FTC will be primarily responsible for enforcement of the Privacy Shield, as it was for enforcement of Safe Harbor, national DPAs in the EU also are given an enforcement role under the program – particularly regarding human resources data of EU citizens that is transferred to the United States. American businesses signing on to the Privacy Shield must agree to cooperate—and even comply—with the direction of national DPAs should an employee complain to his/her DPA about HR data collected in connection with employment. Businesses also may voluntarily submit to the oversight authority of a national DPA, although few are likely to do so.

European Commission Finds Privacy Shield Adequately Protects EU Citizens, Permits Transfer of Personal Data to Certifying US Businesses

On July 12, after nine months of drama following announcement of the ECJ's *Schrems* decision, and despite the well-publicized doubts of members of the Working Party, the European Commission formally declared the Privacy Shield Framework adequate to enable data transfers under EU law (European Commission Decision 2016/1250 of July 12, 2016.) However, the acquiescence of the Working Party, speaking collectively, hardly could be considered a ringing endorsement. The Working Party affirmed that Privacy Shield offers "major improvements" over Safe Harbor, and its statements suggest (i) that it will raise any continuing concerns about Privacy Shield when it undertakes its planned annual review of the program, and (ii) that EU data protection authorities whose members comprise the Working Party do not plan to challenge the program collectively for at least one year.

Although no challenge is expected until at least mid-2017 (if at all) from the Working Party, data protection activists, several political figures, and some individual national data protection authorities, such as the DPA for Hamburg, Germany, have vowed to mount legal challenges to it when practicable to do so. The extremely equivocal support of the Working Party for Privacy Shield, coupled with the avowed opposition of a distinct segment of the data protection community and the directive of the ECJ to DPAs on their obligation to challenge agreements like Privacy Shield if found to threaten privacy rights, do not invest the Privacy Shield with an aura of stability. Yet compared to the alternatives, many U.S. businesses – particularly those that certified to Safe Harbor – will find the Privacy Shield to provide them with the best method for creating and maintaining eligibility to receive data transfers from businesses in EU member states. Careful analysis of options and needs should precede any decision on whether to certify to the Privacy Shield.

Self-Certification Requirements

Self-certification to the Privacy Shield began August 1st. U.S. companies can certify online to the Commerce Department that they comply with the Privacy Shield Principles after conducting and documenting a self-assessment. The Commerce Department reviews the information submitted by each applicant along with the privacy policy they submit, and may also request information regarding onward data transfer agreements. The Commerce Department created a five-step plan

that organizations must satisfy for their self-certifications to be accepted by the agency.

First, they must be eligible to participate. (Banks and telecommunications operators, *e.g.*, are not covered by the program.) Second, they must develop and present a clear, concise privacy policy that includes all of the Privacy Shield principles. Third, the policy must identify the independent recourse mechanism the organization will make available in case of a dispute with a data subject - (typically a U.S.-based arbitration service or agreement to work with European data protection authorities.) Fourth, self-certifiers must specify how they plan to verify they are compliant with the Privacy Shield principles. Finally, the organization must designate a Privacy Shield contact - someone who will be able to respond to complaints within 45 days.

Further information is available on the new website created for the Privacy Shield: https://www.privacyshield.gov/Program-Overview◆

For more information about Schnader's Privacy and Data Security or International Practice Groups or to speak with a member of the firm, please contact:

Scott J. Wenner
Co-chair, International Group
212-973-8115
swenner@schnader.com

Christian Moretti
Co-chair, International Group
212-973-8111
cmoretti@schnader.com

Anne E. Kane
Co-chair, Privacy and Data Security Practice Group
215-751-2397
akane@schnader.com

Stephenie Wingyuen Yeung
Co-chair, Privacy and Data Security Practice Group
215-751-2277
syeung@schnader.com