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

MARCH 2016

PRIVACY SHIELD TAKES ANOTHER STEP FORWARD

By Scott J. Wenner

Roughly three weeks ago EU and U.S. negotiators announced that they had reached agreement on a replacement for the Safe Harbor mechanism for compliance with European regulations on transfers of personal information to the United States. More than 4,000 U.S. businesses were reliant on Safe Harbor to allow them to receive data from Europe on EU-based customers and employees when, in October 2015, it was invalidated by the EU Court of Justice, creating great risk for the businesses that had relied on it. As we reported ***here***, representatives of the U.S. and the EU had already missed the deadline set by European privacy regulators to satisfactorily replace Safe Harbor or see the flow of data to the U.S. cease when a deal was struck even as the deadline in fact passed. The trouble with the February agreement was that the negotiators had nothing to show the regulators beyond an outline of the principles underpinning the deal.

The European regulators' body, known as the Article 29 Working Party ("Working Party"), with which the European Commission ("Commission") must consult on data protection matters, adopted a "wait and see" attitude after the Privacy Shield announcement. However, to avoid a data flow interruption, the Working Party gave U.S. and EU officials an end of February deadline to disclose the details of the Privacy Shield for its review.

On the last day of February, just within the deadline set by the Working Party, the European Commission released the details of the Privacy Shield agreement announced four weeks earlier. Accompanying that text was a draft decision of the Commission declaring that the Privacy Shield will provide adequate protection to the privacy rights of EU citizens whose private information will be transferred to the U.S. under its terms. A decision with respect to the adequacy of a data protection mechanism by the Commission is a predicate under the Data Protection Directive to the lawful transfer of personal data outside the EU.

Simultaneous with the Commission's release of the details of the agreement reached in early February, the U.S. Secretary of Commerce released a set of written commitments signed by the heads of agencies that will have responsibility to enforce the Privacy Shield. This served to underscore the U.S. government's intent to meet the concerns that prompted the EU Court of Justice to invalidate the Safe Harbor accord, including practices of the U.S. intelligence community. Among these materials are 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. Clearly, the production of these commitments were intended to meet and neutralize opposition to and suspicion of the 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.

Indeed, the resemblance of the Privacy Shield framework to the Safe Harbor principles is unmistakable, but largely unavoidable; after all, both require 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.

Resemblance to the Safe Harbor doesn't end with the principles, however. Like the former program, the Privacy Shield program would be administered by the U.S. Department of Commerce, and primary enforcement authority in the United States would reside with the FTC. As noted, the Privacy Shield also is based on self-certification, and businesses would be required to re-certify every year, as was supposed to be the case under Safe Harbor. Addressing a major criticism, U.S. authorities promise this time to more diligently monitor the re-certification process, which some businesses that signed on to Safe Harbor were found to have ignored.

Importantly, 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 principles. It proposes to provide 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 proposed Privacy Shield reserved 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 intelligence agency practices, including providing a specific enforcement mechanism for alleged breaches in the name of national security. The proposal promised the appointment of an ombudsman who would be independent of the intelligence agencies to whom complaints about intelligence oversteps could be directed. (U.S. Under Secretary of State Catherine Novelli was just named as the ombudsman.) In addition, the mechanism contains limitations on access by national security agencies.

As was the case under Safe Harbor, the FTC will be primarily responsible for enforcement of the Privacy Shield, should it be approved. However, national DPAs in the EU also are given an enforcement role under the program – particularly with regard to human resources data of EU citizens that is to be transferred to the United States. American businesses signing on to the Privacy Shield will be required to 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 submit to the oversight authority of a national DPA on a voluntary basis.

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.

While the newly released details of the Privacy Shield and the ancillary commitments of agency

heads are a well-choreographed articulation of a sincere effort by the U.S. government to meet European privacy concerns, whether it will be sufficient to overcome the worries based on the disclosures of NSA surveillance and the perception that Safe Harbor was an empty letter remains to be seen. It is fair to say that the Privacy Shield would toughen monitoring and enforcement; expand remedies and their availability; and create more specific obligations – all assuming that the agencies mean what they say and that certifying businesses do as well. In the meantime, the Working Party will assess the Privacy Shield and present its non-binding opinion, which is expected in mid-April. After that the proposal and the draft adequacy decision can be formally approved (or modified) by the appropriate EU agencies.

Until the EU takes final action, U.S. businesses that certified to the Safe Harbor should continue to comply with that scheme in the interim. While the Working Party has said that it will refrain from taking action against companies that are compliant with Safe Harbor during its review of the Privacy Shield, it observed that national DPAs are free to deem such businesses non-compliant as a matter of national policy. It also would be prudent to look forward and determine how substitution of the Privacy Shield's provisions for the Safe Harbor's will affect businesses that are presently certified to Safe Harbor. ◆

This summary of legal issues is published for informational purposes only. It does not dispense legal advice or create an attorney-client relationship with those who read it. Readers should obtain professional legal advice before taking any legal action.

For more information about Schnader's International or Privacy and Data Security 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

www.schnader.com
© 2016 Schnader Harrison Segal & Lewis LLP
All rights reserved.
** See: www.schnader.com/jakarta*