Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 16, NUMBER 6 >>> JUNE 2016

European Union

Criticisms of Privacy Shield Fail to Recognize Shortcomings of Europe's Own Intelligence Laws

By Julie Brill and Winston Maxwell

Unveiled Feb. 29, 2016, the new European Union-U.S. Privacy Shield attempts to address the shortcomings of the U.S.-EU Safe Harbor arrangement identified originally by the European Commission and later by the Court of Justice of the European Union (CJEU) in its *Schrems* decision (*Schrems v. Data Prot. Comm'r*, E.C.J., No. C-362/14, 10/6/15). The Privacy Shield proposes improved data protection principles, better enforcement by the U.S. Department of Commerce and the Federal Trade Commission (FTC), redress mechanisms for EU citizens and safeguards surrounding law enforcement and intelligence activities. Like Safe Harbor, the Privacy Shield is a co-regulatory system: companies that want to participate in the system agree to a set of data protection principles, and implement those principles within their organization under the supervision of the regulator—in this instance the U.S. Department of Commerce and the FTC.

This approach is similar to Binding Corporate Rules (BCRs) or the data privacy governance certificate "proposed by France's data protection regulator, CNIL. Companies that agree to the principles are accountable for their implementation within their corporate group. Companies must be prepared to demonstrate to authorities the measures taken to ensure compliance. This is an example of the accountability principle encouraged by the new General Data Protection Regula-

tion 2016/679 (GDPR). In that respect, the Privacy Shield is consistent with European regulatory trends as expressed in the GDPR.

European Privacy Shield Opinions.

The Article 29 Working Party of data protection officials from the 28 EU member states issued an opinion on April 13, 2016 expressing concerns about Privacy Shield's adequacy (16 WDPR 04, 4/28/16). The European Parliament adopted a resolution on May 26, 2016 praising the progress made, but highlighting shortcomings in the Privacy Shield as presented in February 2016 . The European Data Protection Supervisor (EDPS), Giovanni Buttarelli, issued an opinion on May 30, 2016 stating that the current Privacy Shield proposal required "robust improvements" (16 WDPR 06, 6/28/16). Now that the Irish Data Protection Controller has referred another data transfer mechanism known as Standard Contractual Clauses to the courts for review of their adequacy, greater focus will be placed on whether the criticisms of Privacy Shield are well founded .

The European Parliament, Article 29 Working Party and the EDPS unanimously criticized the powers of U.S. intelligence agencies, arguing that they violate the proportionality principle of the Charter of Fundamental Rights of the European Union. These European observers disparage the vague definition of "foreign intelligence" in U.S. legislation, and the potentially large scale of signals intelligence activities, including on submarine cables. But crucially, the criticisms relating to proportionality of intelligence gathering also apply to similar powers available in Europe, yet these European intelligence powers go unmentioned.

EU Versus U.S. Surveillance.

The broad powers accorded to intelligence agencies in the U.S. and Europe raise sensitive issues relating to the proper balance between privacy and national security. Civil rights advocates have criticized the U.S., but also European governments, for having increased the powers of intelligence agencies without adequate privacy safeguards. One of Europe's top human rights officials, Nils Muisnieks, criticized governments in the EU for the extensive powers granted to national intelligence agencies to gather data about EU citizens. The European Parliament adopted a resolution on Oct. 29, 2015 warning of the dangerous "downward spiral" in Europe of anti-terrorism laws granting broad powers to intelligence agencies, with little or no independent supervision.

With its recent laws on intelligence gathering and on interception of communications outside of France, France follows this trend. France still imposes broad data retention obligations on telecommunications operators and Internet service providers, even though the European Directive on which those obligations are based was invalidated by the European Court of Justice in 2014 in the *Digital Rights Ireland* case . France's anti-terrorism laws permit bulk untargeted collection of metadata using so-called black boxes, in order to identify patterns that may lead to terrorist plots. France's recent law confirms intelligence agencies' ability to intercept communications and collect metadata regarding communications received or sent outside of France whenever necessary to protect "France's fundamental interests." This activity is subject to minimal oversight, as long as no French telephone numbers are involved. This aspect of French law provides lower protection to non-French residents than to French residents, which is precisely one of the criticisms leveled at the U.S. system.

The U.S. legal framework for intelligence gathering balances protection of individual rights and national security interests in a manner that's similar to the balance struck in several European countries.

Granting more power to intelligence agencies is understandable in light of the heightened terrorist threat in France and elsewhere in Europe. What is more surprising is that the European authorities analyzing Privacy Shield criticize the U.S. system without referring to the intelligence gathering powers of authorities in Europe, which in many cases suffer from the same shortcomings as those singled out for criticism in the U.S. system.

The U.S. legal framework governing intelligence gathering activities balances protection of individual rights and national security interests in a manner that is similar to the balance struck in several European countries, including France. Like French law, U.S. law makes a distinction between gathering data in the context of criminal procedures, and gathering data in the context of intelligence activities. Data processing in the context of criminal investigations is generally surrounded by a high level of protection for individual rights, both in France and in the U.S. European residents are now even more protected with the enactment of the "Judicial Redress Act," which gives Europeans certain procedural rights that had been, prior to the Act, only available to U.S. residents.

The harder issues reside in intelligence gathering activities. The Article 29 Working Party and the EDPS criticize the lack of clarity in U.S. law relating to the definition of "foreign intelligence" and "foreign intelligence information." But the U.S. definitions are no less precise than the broad definitions appearing in France's Internal Security Code, which allow surveillance for, among other things, protection of France's "major economic interests." In addition, the Working Party recognized the existence of effective internal controls within U.S. intelligence agencies, but criticized the U.S. for not having stronger independent oversight, preferably by a judge. Here too, the U.S. situation is no different from France's, where intelligence gathering activities are overseen by a National Oversight Commission on Intelligence Gathering Techniques, whose opinions are not binding on the Prime Minister. The European authorities criticize bulk collection of data, yet France's intelligence law allows intelligence authorities to conduct data mining over huge volumes of metadata.

   ISSN 1473-3579

Do What We Say, Not What We Do.

In summary, the Working Party, European Parliament and EDPS criticize the U.S. intelligence gathering system because it does not correspond to a European ideal of protection of individual liberties in the context of intelligence activities, even though in many parts of Europe, this European ideal is not reflected in the national laws adopted to facilitate intelligence gathering. Like parents speaking to their children, the Working Party essentially opines "do what we say, not what we do."

In reality, the Privacy Shield includes several measures that improve the protection of Europeans with respect to intelligence gathering activities, including a new right of indirect access similar to what exists in France. A person who wants to know whether his or her data are collected by U.S. intelligence authorities would be able to make a request to his or her local DPA, who would forward the request to a high-ranking official—called an "Ombudsman—within the Department of State. The Ombudsman would in turn verify that any surveillance measure has been implemented in accordance with law. As in France, the U.S. ombudsman would not generally be able to confirm whether a person is listed in an intelligence file, since that information would be classified. But the Ombudsman would verify that appropriate procedures have been followed, and correct any anomalies. This too is similar to the system that exists in France for data included in intelligence data bases. Notably, the Ombudsman is only available to Europeans, and not to U.S. citizens. In addition, the U.S. government has agreed to apply to Europeans most of the same protections as those that exist for U.S. citizens.

In reality, the Privacy Shield includes several measures that improve the protection of Europeans with respect to intelligence gathering.

Some of these criticisms may be taken into account by the European Commission and the U.S. government as they finalize their negotiations over Privacy Shield and prepare its final documentation. The EDPS made several pragmatic suggestions on how to improve the current proposal, such as by requiring the U.S. Ombudsman to report to Congress. However, other criticisms, such as those relating to the lack of a precise definition of "foreign intelligence" under U.S. law, may both be difficult and unnecessary to address.

The European Commission will likely issue its decision on the "adequacy" of the Privacy Shield sometime this summer, and from that point onward, the Privacy Shield will become legally operational for data transfers. However, some DPAs, in particular in Germany, have indicated that they will challenge the Privacy Shield in court, which could lead to a new referral to the CJEU. Consequently, despite the fact that the Privacy Shield presents essentially equivalent protections to the protections available to EU citizens under European law and should be deemed adequate by the CJEU, the status of the Privacy Shield as a robust data transfer mechanism may remain uncertain for some time to come.