Privacy Shield's Prospects: The Good, the Bad, and the Ugly

By **Peter Margulies**
Thursday, March 3, 2016, 8:50 AM

Link: https://www.lawfareblog.com/privacy-shields-prospects-good-bad-and-ugly

If the devil is in the details, then the announcement early Monday of the inner workings of the new US-EU data-transfer agreement, Privacy Shield, may lack the granularity the deal needs to flourish. There is much to applaud in the new agreement, including extraordinary transparency from the US and a new safeguard to address EU privacy complaints in the form of a State Department Ombudsperson. Those virtues, however, may not be sufficient to ensure the viability of Privacy Shield, which replaces the Safe Harbor framework invalidated by the Court of Justice of the European Union (CJEU) in *Schrems v. Data Commissioner*.

The CJEU struck down Safe Harbor on the grounds that it lacked both substantive and independent procedural protections against US intelligence collection. The Privacy Shield roll-out is short on concrete information regarding the State Department Ombudsperson's authority and is instead reliant on broad US "representations" regarding substantive limits on foreign intelligence collection. The CJEU may not be impressed, especially since the CJEU rarely provides European officials with the deference supplied by the European Court of Human Rights (ECHR).

First, the good in Privacy Shield: ODNI General Counsel Bob Litt's letter reinforces a salutary trend toward transparency that ODNI has championed since the Snowden revelations. To my knowledge, no intelligence service has provided close to the level of detail about intelligence community (IC) structure and decision making that the ODNI letter provides, as it builds on the commitment announced by President Obama in his PPD-28 initiative. The ODNI letter painstakingly describes several layers of review within the IC, including the setting of priorities by the National Signals Intelligence Committee (SIGCOM). In comparison, most European states continue to keep mum about their own internal processes.

The ODNI letter also reaffirms substantive limitations in PPD-28. Bulk collection abroad, which ODNI says may sometimes be necessary to "identify new or emerging threats" concealed in the forest of global data, is limited to the grounds specified in PPD-28, including counterterrorism, combating weapons proliferation, addressing transnational illegality including sanctions evasion, detecting threats to US or allied forces, and learning about certain activities of foreign powers. The US also reiterates its PPD-28 pledge not to collect information in bulk for the purposes of suppressing dissent, disadvantaging individuals or groups based on criteria such as race, gender, or religion, or supplying US firms with a competitive advantage. Moreover, the IC cannot engage in the "arbitrary or indiscriminate collection" of data regarding "ordinary European citizens."

The ODNI letter commits the IC to tailoring collection. Analysts will focus on "specific foreign intelligence targets or topics through the use of discriminants (e.g., specific facilities, selection terms and identifiers)" whenever that specific approach is "practicable." Moreover,

the IC has multiple layers of internal review, including the ODNI Civil Liberties and Privacy Office. I would add that my own conversations with ODNI and NSA privacy officials—who regularly engage with the public and the privacy community—reinforce my view that this internal control is indeed robust. Other constraints within the executive branch include inspectors general who report regularly to Congress, and the Privacy and Civil Liberties Oversight Board (PCLOB), which has authored well-received reports on U.S. surveillance. In addition, ODNI notes that the Foreign Intelligence Surveillance Court (FISC) now has statutory authority to appoint independent advocates, including noted privacy advocates. And, of course, Congress can also monitor the IC, exerting budgetary pressure if it sees something untoward. The FISC's authority to appoint independent attorneys stems from statutory changes, including the USA Freedom Act, negotiated with the Administration in the wake of Snowden's disclosures.

That's the good in the Privacy Shield roll-out; now for the bad. First, the US representations that it won't engage in "arbitrary or indiscriminate" collection on Europeans are described only in general terms. The European Commission (EC) statement that the new framework has "adequate" protections for Europeans relies on "explicit assurances" provided by the US. However, the EC statement shares nothing on what those assurances entail. Since the US and the EC have significant business interests dependent on a new privacy agreement, some may question whether those assurances are as robust as the CJEU or EU privacy regulators would prefer. There is simply no way to judge, based on the materials disclosed thus far.

Moreover, the ODNI letter does not address a central EU concern with the status quo: the vagueness of the "foreign affairs" basis for collection under section 702 of the Foreign Intelligence Surveillance Amendments Act (for more, see Tim Edgar's analysis). I've written previously that the foreign affairs prong of section 702 is limited by language that confines such collection to matters concerning a "foreign power" or "territory." I continue to believe that this language focuses the foreign affairs prong on collection relating to foreign officials and does not extend to monitoring of foreign persons' routine activities. Perhaps the assurances that US officials provided to the EC confirm this view. Moreover, perhaps the FISC can provide a check to unduly broad interpretation of this provision, since the EC adequacy analysis states that the IC has agreed to a PCLOB recommendation to provide the FISC with a random sample of analysts' tasked searches. However, the lack of public reassurance on this score underlines a concern of the EC Working Group that the CJEU highlighted in Schrems.

Furthermore, procedural safeguards outlined by ODNI may not be as robust as the CJEU wishes. The inspectors general, for example, are hampered by a recent Justice Department Office of Legal Counsel opinion that allows executive branch agencies to limit disclosure of data to inspectors general conducting investigations. Moreover, the FISC has no control over the United States' biggest foreign collection program, which is based on Executive Order 12333. The State Department Ombudsperson may have the authority to address complaints that involve EO 12333, but the announcement is not clear on this point. The Ombudsperson description in Annex III of the roll-out says that this official will "work closely" with other government officials. Nevertheless, the description does not specify that the Ombudsperson will have full access to IC data and procedures.

Similarly, according to the EC statement, the Ombudsperson will have to "confirm" that each complaint received has been "properly investigated." To confirm this, the Ombudsperson must ascertain that surveillance has complied with US law, including the "representations"

and “explicit assurances” that the US has provided, or that any violation has been remedied. However, this confirmation brings us back to the lack of specificity in the public version of those US “representations.” It is difficult to see how robust the Ombudsperson’s review will be, when so much depends on assurances that are not accessible to the public, the CJEU, or European data regulators.

As Privacy Shield is implemented, the Ombudsperson may develop a course of dealing with the IC that addresses these concerns. Experience might demonstrate that the Ombudsperson has access to all the information that she needs, and uses that information to keep the IC honest. But that experience will be outside of the four corners of the Privacy Shield’s founding documents, making consideration of experience’s teachings a tougher sell with skeptical actors such as the CJEU.

That brings us to the ugly. The CJEU should provide some deference to the EC, particularly on matters involving national security. That deference is apparent in decisions of the ECHR on surveillance, such as *Weber v. Germany*, which upheld a substantial overseas surveillance program conducted by the German Republic. However, the CJEU has in practice diminished deference to near-microscopic levels in cases like *Schrems* and *Kadi v. Council*, which invalidated the EU’s implementation of the UN’s terrorist sanctions framework. Indeed, the framework invalidated in *Kadi II* also involved an ombudsperson, who had been effective in ensuring fairness to subjects of sanctions. This real-world efficacy made no difference to the CJEU. Instead, the CJEU insisted on a more formal due process mechanism, which was unworkable because of states’ reluctance to disclose intelligence sources and methods supporting terrorist designations.

The CJEU may also have concerns about the independence of the State Department Ombudsperson for Privacy Shield. True, that official will not formally be part of the IC, and in this sense will be independent. Nevertheless, the State Department is also an executive branch department, and is a customer of the IC, making use of intelligence that the IC provides. The President can fire the Ombudsperson, as he or she can fire IC officials. The Ombudsperson may as a practical matter retain independence, as inspectors general do, because of her different constituency. But that belief hinges on institutional culture more than formal legal guarantees. Institutional culture may be too weak a reed to support Privacy Shield, particularly for a court as activist as the CJEU.

In sum, Privacy Shield brings much to the table, including a welcome US candor that will hopefully rub off on our more reticent European allies. The Ombudsperson proposal has significant promise. However, it is too early to tell whether the Ombudsperson can develop a track record of effectiveness that persuades the CJEU and European regulators who found Safe Harbor wanting.