Safe Harbor 3.0 – What it Says May Be Less Important than Where it Gets Adjudicated

David Bender

Introduction – In striking down Privacy Shield on July 16, 2020 (the "Schrems II" decision), the European Union's highest court – the Court of Justice of the EU (the "CJEU") - found two deficiencies in US national security surveillance: its perceived overreach and lack of proportionality, and its lack of redress for wronged EU residents.

It appears from public statements that the United States and the EU intend to find a Privacy Shield successor. Presumably, the US will is in some way to modify its laws regarding surveillance and redress for EU residents, the parties will once more negotiate a unique vehicle (it's being called "Safe Harbor 3.0") for export to the US, and they will then seek an adequacy decision from the European Commission. Any such adequacy decision will be challenged immediately. The thesis of this article is that such an adequacy decision is more likely to survive if adjudicated in a court other than the one that invalidated Privacy Shield and Safe Harbor. And there may be such a court with jurisdiction.

Commissioner Reynders' Quest -- In September I viewed a webcast that featured Didier Reynders, the EU Commissioner of Justice. Commissioner Reynders heads the EU delegation deliberating with a United States Department of Commerce team in attempting jointly to fashion Safe Harbor 3.0. He was speaking about post-*Schrems II* export of personal data from the EU, and the proposition underlying his remarks caught my attention. What we are trying to do for EU personal data, he proclaimed several times, is to retain, after it leaves the EU, the protection that it has in the EU. The context of his remarks was national security surveillance, the bugaboo that brought down Privacy Shield, just as it had previously invalidated Safe Harbor.

Retaining protection for personal data is obviously a legitimate goal. Nevertheless, the Commissioner's proclamation rings hollow, because it incorporates an inaccurate assumption: namely, that as to national security surveillance, the data was relatively well-protected in the EU to begin with. That presumption flies in the face of numerous analyses that have compared national security laws around the world. Study after study has shown that the sensitivity to privacy embodied in US surveillance law is exceeded in the laws of few if any nations – including EU Member States. For example, in 2018, a top EU court held that surveillance provisions embodied in the UK's Investigatory Powers Act 2016 violated the European Convention on Human Rights. And in July of this year the German Constitutional Court held that the German intelligence service was applying bulk surveillance techniques to foreigners in violation of the German constitution. Insofar as legal protection against governmental surveillance is concerned, on the whole, the EU data about which Commissioner Reynders is concerned is in fact better-protected once it hits the US than it was before it was sent.

Schrems II -- That fact was not something with which the CJEU concerned itself (or even acknowledged) in rendering *Schrems II*. The court decided that the appropriate yardstick for measuring the propriety of US surveillance law was EU law, *i.e*., the General Data Protection Regulation interpreted in light of the Charter of Fundamental Rights of the European Union. And, in particular, it decided that the surveillance law of the Member States is not the appropriate yardstick. In fact, the surveillance law of few if any Member States measures up to the requirements of EU law -- the court's chosen yardstick. Nor did the court trouble itself with the possibility that, if few nations meet its standard, perhaps that should be a major consideration in the required balancing between data protection and national security.

Indeed, some would argue that the CJEU is caught in a time warp, and cannot seem to get past June 5, 2013, the day on which Edward Snowden made his revelations. Snowden's disclosures enraged countless Europeans (as well as many in the US), and for some, that indignation continues to this day. So some observers would contend that the CJEU seems (1) fixated solely on the Charter's data protection provision, (2) indifferent to crediting legitimate concerns about terrorism, (3) oblivious to developing a realistic yardstick for measuring permissible surveillance intrusion into privacy, and (4) uninterested in meaningfully complying with the Charter's mandate of proportionality.

What Now? -- The conventional wisdom is that if we are to promulgate a successful Privacy Shield follow-on, US surveillance law must be modified. And that if the modification is significant enough, the third time around will be the charm, and in due course the CJEU will approve the adequacy decision. Yet a significant modification may not be easy to effect. If truth be told, some commentators question whether there should be any such modification at all. In fact, a former NSA general counsel argues that it is time for the US to show the EU that the US has "the right to write U.S. laws without getting permission from European governments."[1]

The Charter and the CJEU -- The Charter - which has constitutional stature in the EU - does indeed mandate data protection, but also requires that it be balanced against other important rights, such as national security (the European term for this balancing is "proportionality"). The Charter states: "Subject to the principle of proportionality, limitations [on rights recognized by the Charter] may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."

But the CJEU has generally given short shrift to proportionality when data protection rights are involved (and not merely with regard to Safe Harbor and Privacy Shield). Instead, the CJEU has used as its yardstick for permissible national security surveillance a rather rarified standard. The CJEU did not consider the relative privacy-sensitivity of US surveillance law in establishing a benchmark against which to measure

---

[1] S. Baker, "How Can the U.S. Respond to Schrems II?", Lawfare (July 21, 2020), available at <lawfareblog.com/how-can-us-respond-schrems-ii>.

permissible surveillance levels. Rather, the CJEU insisted that US national security meet standards that most Member States do not meet. Thus, the court told the US to "do as we say, not as we do." The structure of EU and Member State law may compel such a position. But if the EU is truly concerned about national security's encroachment into privacy, one wonders why the EU has not cleaned up the Member State stables. Or why the EU did not challenge transfers to authoritarian nations, such as China or Russia, before tackling transfer to the US.

A Possible Alternative -- Another instrument regarded as having constitutional stature in all EU Member States is the European Convention on Human Rights (the "Convention"). It is actually an instrument, not of the EU, but of the Council of Europe ("COE"), another European institution. The COE has 47 Member States, including all 27 EU Member States. Like the Charter, the Convention creates data protection rights and requires proportionality as between those rights and other important values (like national security). But here's the critical difference – alleged violations of the Convention are not adjudicated in the CJEU; they are adjudicated before the European Court of Human Rights ("ECtHR"), a court with stature similar to that of the CJEU.

The sole purpose of the ECtHR is to ensure that COE Member States respect the rights and guarantees set out in the Convention. Whereas the CJEU is the final enforcer of the Charter, the ECtHR is the final enforcer of the Convention. Data protection is dealt with prominently in both instruments, and has been the focus of many decisions in each court. Moreover, the Charter states: "In so far as this Charter contains rights which correspond to rights guaranteed by [the Convention], the meaning and scope of those rights shall be the same as those laid down by the said Convention."

The CJEU stated in *Schrems II* that (i) the Convention is not a part of EU law because the EU itself has not acceded to it (although all of its Member States have), and (ii) CJEU precedent held that the CJEU must interpret EU law in light of the Charter. But in fact, by virtue of the language quoted in the preceding paragraph, the Charter requires the CJEU to construe the meaning and scope of rights guaranteed in both instruments "the same as those laid down by the Convention." Presumably, that means the same as construed by the ECtHR. In other words, by virtue of the quoted language from the Charter, the ECtHR's construction of rights guaranteed in both the Charter and the Convention *is deemed to be* EU law.

Similar Issues, Different Results -- An examination of decisions in each court involving conflicts between data protection and national security reveals something interesting: the ECtHR is more likely to rule in favor of national security than is the CJEU. The CJEU tends to view any national security law impinging on data protection as violating the Charter. But the ECtHR actually engages in a meaningful balance of data protection against national security, and not infrequently finds that the national security law in question did not contravene the Convention. In fact, had the Privacy Shield adequacy decision been challenged in the ECtHR, well, who knows how it would have turned out.

The Conclusion – The expectation is that the validity of any Safe Harbor 3.0 adequacy decision will ultimately be adjudicated in the CJEU. Whatever change the US

is willing to make in its surveillance law (if any) may or may not suffice for the CJEU. But the chances for an affirmative ruling would be enhanced if the matter were adjudicated instead in the ECtHR. Could that happen? I don't know. Certainly, there would be a footrace between two groups, each trying to get its case heard in the court of its choice. Among the legal issues that would have to be considered are the following:

- the mechanics of bringing suit under each of the two instruments,
- how to accelerate cases to reach each of the two forums (neither of which is a court of original jurisdiction),
- precise precedential value in either court of a decision in the other, and
- likelihood that the ECtHR would view *Schrems II* as precedent precluding a different result for Safe Harbor 3.0.

But this alternative might be worth pursuing, as the forum in which Safe Harbor 3.0 is adjudicated may be every bit as important as its content.