The Sinking of the Safe Harbor

Christopher Kuner

08.10.2015 doi: 10.17176/20170330-152012

The judgment of the Court of Justice of the European Union (CJEU) in *Schrems v. Data Protection Commissioner* (Case C-362/14) is a landmark in EU data protection law, but one about which I have serious misgivings. While I share the Court's concern regarding the surveillance practices of the US government (and other governments for that matter) and some of its criticisms of the EU-US Safe Harbor Arrangement, I take exception to its lack of interest in the practical effects of the judgment and the global context in which EU law must operate.

The judgment largely affirms the opinion of Advocate General Bot of 23 September, and holds that the national data protection authorities (DPAs) must have the power to reach their own conclusions about European Commission decisions concerning the adequacy of data protection in third countries under Article 25 of EU Directive 95/46 (paras. 38-66 of the judgment). In finding Commission Decision 2002/520 establishing the Safe Harbor to be invalid (para. 106), the Court affirms the need for a high standard of data protection as set out in its previous case law such as Digital Rights Ireland (Joined Cases C-293/12 and C-594/12), and holds that while data protection standards in third countries need not be "identical" to those in the EU, they must be "equivalent" (para. 73). It goes on to conclude that US law fails to limit interference with EU fundamental rights (para. 88), and that Decision 2002/520 contains gaps in protection with regard to data transferred under the Safe Harbor (para. 89).

As the Commission stated in the Communication introducing its proposed General Data Protection Regulation (GDPR) that will replace the Directive, the current fragmentation of data protection law in the EU has already led to "uneven protection for individuals", and the Court's confirmation that individual DPAs may interpret Commission decisions (para. 53) will only make the situation worse. The judgment's emphasis on the need for the DPAs to be "completely independent" (see paras. 40, 57, and 99) will complicate the adoption of a legal framework for their cooperation in the proposed European Data Protection Board foreseen in the GDPR.

The judgment also creates uncertainty concerning data transfers conducted under other legal mechanisms (e.g., standard contractual clauses or binding corporate rules). The Court stresses that adequacy must be determined based on the "domestic law and international commitments" of a third country (para. 96), suggesting that it depends not just on the details of particular data transfer mechanism, but on the totality of fundamental rights protection in a third country's legal system.

Since these other data transfer mechanisms grant no greater protection against access by the intelligence services than did the Safe Harbor (as I have argued previously), the judgment implicitly seems to throw them into question as well. Indeed, many or perhaps even most countries around the world exempt the activities of their intelligence services from their national data protection law and lack an effective oversight structure for surveillance activities, leading one to ask how under the Court's reasoning adequate protection for data transfers can ever exist.

Thousands of former Safe Harbor member companies (including those with their headquarters in the EU) will now have to begin a lengthy process to implement alternative mechanisms for transferring data to the US, creating a legal vacuum for the protection of data transfers. The fact that the Court failed to use its power, which it has exercised on other occasions (see Société Regie Networks, Case C-333/07), to mitigate the temporal effects of the judgment and give companies a "grace period" to implement alternatives to the Safe Harbor shows its lack of interest in how EU data protection law functions "on the ground".

Motivating third countries to adopt EU data protection standards requires that the bar not be set so high that they have no realistic chance of meeting it. The CJEU has held that EU law is an autonomous and unique legal order (see Opinion 2/13, para. 158), suggesting that by definition few countries outside the European region will be able to emulate it.

Setting an unrealistic standard for adequacy and inciting individuals to have adequacy decisions reviewed by the CJEU (see paras. 61-65) makes a system that is already slow and cumbersome, with only 12 decisions issued in 17 years (11 minus the Safe Harbor), even more glacial. The issuance of adequacy decisions by the Commission has become an example of what Martti Koskeniemi refers to as human rights "petrified into a legalistic paradigm", and has little to do with real data protection. It is hard to understand why the EU legislator has apparently not included any improvements to the process for issuing adequacy decisions (which could include, for example, deadlines, greater transparency, input from stakeholders, etc) in the GDPR.

The Court could have required reform of the Safe Harbor while still upholding fundamental rights, such as by adopting a *Solange* approach coupled with a demand to make improvements within a certain time period. Instead, it makes the transfer of personal data to third countries dependent on their strict adherence to EU standards, which is not feasible in a pluralistic world with over two hundred countries and many different conceptions of rights.

The late Ulrich Beck wrote that "in order to pursue their national interest, countries need to...surrender parts of their autonomy in order to cope with national problems in a globalized world". Data protection is a prime example of an area of law where national and local approaches are no longer sufficient. The EU and the US share deep cultural and historical ties, and as liberal democracies their legal systems have many similarities. In theory, providing legal protection for data transfers across the Atlantic should be one of the easier tasks of privacy lawmaking, and if we cannot do this, then how can it ever be provided for data transfers to countries like China and India? The idea that EU data protection law can survive in a constitutional biotope walled off from contact with other legal systems is illusory, and will only undermine the global protection of personal data that the *Schrems* judgment aims to promote.

ABOUT THE AUTHOR

Christopher Kuner

Dr. Christopher Kuner is Affiliate Professor at the University of Copenhagen, Associate of the Centre for European Legal Studies of the University of Cambridge, Senior Privacy Counsel in the Brussels office of Wilson Sonsini Goodrich & Rosati, and Visiting Fellow at the Maastricht European Centre on Privacy and Cybersecurity of Maastricht University.Dr. Christopher Kuner is Affiliate Professor at the University of Copenhagen, Associate of the Centre for European Legal Studies of the University of Cambridge, Senior Privacy Counsel in the Brussels office of Wilson Sonsini Goodrich & Rosati, and Visiting Fellow at the Maastricht European Centre on Privacy and Cybersecurity of Maastricht University.

SUGGESTED CITATION

Kuner, Christopher: The Sinking of the Safe Harbor, Verfassungsblog, 08.10.2015, doi: 10.17176/20170330-152012.

Licensed under CC BY-SA 4.0.

Langzeitarchiviert bei IntRechtDok unter: doi.org/10.17176/20170330-152012.