European Law Blog

Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy Negotiations (Part 1)

Theodore Christakis

European Law Blog

Published on: Apr 12, 2021

URL: https://europeanlawblog.pubpub.org/pub/squaring-the-circle-international-surveillance-underwater-cables-and-eu-us-adequacy-negotiations-part1

Part 1: Countering the U.S. Arguments

As the United States (US) and the European Union (EU) "intensify" negotiations to reach a new adequacy decision following the invalidation of Privacy Shield by the Court of Justice of the European Union (CJEU) in its July 16, 2020 *Schrems II* judgment (discussed here, here and here), one pressing question is what should be *included* and what should be *excluded* from the scope of the negotiations. It went unnoticed, but the US submissions to two recent European public consultations (one by the European Commission and another one by the European Data Protection Board (EDPB)) on post-*Schrems II* developments provide a glimpse of what could become a thorny issue during the ongoing EU-US negotiations for a successor to Privacy Shield.

More precisely, this thorny issue is whether *international* surveillance, conducted by US intelligence agencies *outside* the territory of the US on the basis of Executive Order 12333 (EO 12333)[1], should be (or not) part of the adequacy assessment. The EU seems to consider that excluding international surveillance and EO 12333 from the scope of the successor to the Privacy Shield adequacy decision would be problematic and could give the impression of trying to "re-litigate" the Schrems II judgment, with all the risks that this could involve for a future invalidation by the CJEU of a new adequacy decision in a "Schrems III" case. The US, in contrast, disputes this approach, talks about "double standards" and seems to consider that EU demands about US international surveillance limitations go far beyond what is required by EU law and what is practiced by EU Member States themselves in their international surveillance activities.

This article will be published in two successive parts.

In **Part 1**, published here, I will present the US arguments which intend to exclude from the scope of the EU-US negotiations all "direct access" to data by US intelligence agencies. I will explain that what is basically at stake here is international surveillance and the effort to exclude Executive Order 12333 from the scope of the adequacy assessment. I will then present four possible responses to the US arguments, based especially on the role that the European Convention of Human Rights (ECHR) could play in this field and on a teleological interpretation of the General Data Protection Regulation (GDPR).

In **Part 2**, which will be published here tomorrow morning, I will enter into a critical approach of the EU position on the relevance of the ECHR and I will argue that the US could reasonably put forward an equally strong and legitimate number of counter-arguments. I will also present a series of thoughts and proposals that could help the two sides to get out of this mess in a satisfactory way while achieving what is really required by EU law: protection of EU personal data wherever they are, in Europe, in the US or in transit in submarine transatlantic cables.

The US position: Adequacy should exclude direct access

Using the CJEU *Privacy International* and *La Quadrature du Net* judgments on data collection/retention of October 6, 2020 (see analysis here) as a point of departure, the US argues (here at 7-11 or here at 5-8) that surveillance *directly undertaken* by US intelligence agencies should remain *out of the scope* of standard contractual clause (SCC) assessments by data exporters on whether US surveillance laws offer a level of protection "essentially equivalent" to that which exists within the European Union. Similarly, and logically, the ongoing EU and US adequacy negotiations should exclude from their scope the issue of direct access to data by US intelligence agencies and should only focus on US surveillance laws that authorise US authorities to request disclosure or processing of data by service providers.

The US claims that assessments on whether US surveillance laws offer a level of protection "essentially equivalent" to that guaranteed within the European Union should clearly distinguish between two different types of government access to data: **indirect or compulsory access** on the one hand, i.e. situations where a government compels electronic communications service providers to turn over communications to the government or to authorize access in their networks; and **direct or non-compulsory access** on the other hand, i.e. situations where the government collects the data directly by its own means without any compelled disclosure or processing of data or even awareness by a private actor. According to the logic of the US, while "adequacy/essential equivalence" assessments are relevant for the first type of access to data by intelligence agencies, the second type of access should be excluded from the scope of such assessments.

The basic argument used by the US to back this claim is that EU data protection law *does not apply* in relation to direct access to data by intelligence agencies for national security purposes, when such access does not impose data processing obligations on private entities. The US claims that "requiring assessments of this type of data access is inconsistent with recent judgments by the Court of Justice, would impose an impossible burden on data exporters, and would make data flows subject to disruption based on rumors and conjecture." (here at 8).

The US focuses on the interpretation of the "national security exception" in EU data protection law given by the CJEU in its October 6, 2020 data collection/retention judgments. It should be recalled that in these cases NGOs challenged in domestic courts the collection of bulk communications data and data retention provisions. *Privacy International* challenged the collection of bulk communications data by UK intelligence agencies under UK surveillance law and *La Quadrature du Net* (*LQDN*) challenged the data retention provisions of French surveillance law. The cases were then referred to the CJEU by the UK and French courts. The CJEU held that, while the "national security exception" in EU law *does not* apply when EU Member States seek to impose obligations (to transfer or retain data) on electronic communication service providers in the name of national security, it *does apply* each time intelligence agencies *process data themselves* for national security purposes, thus excluding such activities from the scope of EU law. The US therefore concludes that:

> "In sum, under *LQDN* no EU legislation governs direct access by Member State authorities to personal data for national security purposes—not the e-Privacy Directive, not GDPR, and not the Law

> Enforcement Directive. Since EU law provides no privacy protections relating to EU Member State governments' direct access to personal data for national security purposes, a data exporter would have no comparative standard by which to assess whether privacy protections offered by a destination country for the same type of activities are "essentially equivalent" to protections required by EU law. The EDPB should not interpret *Schrems II* to create a double standard under which non-EU countries' direct access measures are subject to strict EU data protection rules while comparable Member State direct access measures are not subject to EU law at all." (here at 9).

Aside from referring to CJEU data collection/retention judgments, the US advances the argument that fairness should prevail, and that democratic and transparent countries could be "punished" if direct access is taken into consideration in adequacy/essential equivalence assessments. According to the US:

> "Requiring data exporters to take into account this type of data access would have the perverse result of punishing countries like the United States that have taken substantial measures towards transparency and rewarding others who have chosen to keep their involvement in such activities entirely secret. Perhaps most troubling, non-democratic, authoritarian regimes that obtain non-compulsory direct access not only to data outside their territory, but within it as well, with no public transparency whatsoever, would be in a more favorable position under EU law than transparent democracies." (here at 10, notes omitted).

Explanation: It's all about Executive Order 12333 and international surveillance

One wonders *why* the US insists on excluding direct or non-compulsory access to data by governments from the scope of adequacy/essential equivalence assessments. The objective, as described in the US submissions, is to make a clear distinction between the two US surveillance authorities discussed in the Schrems II judgment, namely Section 702 of the Foreign Intelligence Surveillance Act (FISA 702) and Executive Order 12333 (EO 12333).

On the one hand, FISA 702 authorises US intelligence agencies, subject to a series of conditions, to *compel* service providers to disclose data and should thus be covered by adequacy/essential equivalence assessments.

EO 12333, on the other hand, does not give any power to US authorities to compel disclosure or other processing of data by service providers.[2] It only concerns "direct surveillance" in terms of providing a framework[3], under certain conditions, for US intelligence agencies to access electronic communications *outside* the United States or data in transit.[4] For instance, consistent with EO 12333, the NSA can access the underwater cables on the Atlantic Ocean floor, by means of which data are transferred from the EU to the US, *before* they arrive in the US and become subject to the provisions of the FISA. Despite the absence of an official US acknowledgment of such interceptions (see discussion in Part 2 to be published tomorrow), the Snowden revelations showed that this is not just a theoretical possibility. Following these revelations, the Obama administration adopted in 2014 Presidential Policy Directive 28 (PPD-28), which applies to all

activities involving the collection and use of foreign intelligence signals information, including EO 12333. PPD-28 provides that respect for privacy is an integral part of the considerations to be taken into account in the planning of those activities, that the collection must be aimed solely at the acquisition of foreign intelligence information and counter-intelligence and that the activities must be "as tailored as feasible". However, in *Schrems II* the CJEU pointed to several weaknesses of PPD-28 from the point of view of EU law (see §§ 181, 183, 184 and 192 of the judgment).

The US might feel that it would be easier to address the deficiencies in US surveillance law (proportionality and judicial redress) highlighted by the CJEU in *Schrems II* with FISA 702 rather than EO 12333. The exclusion of EO 12333 from the adequacy/essential equivalence equation could thus be helpful for the US in order to reach an agreement with the EU and allow transatlantic data flows. Furthermore, it is difficult for the US to understand why its international surveillance activities would be placed under close scrutiny by the EU, when international surveillance by EU Member States themselves (including access to underwater cables[5]) is entirely excluded from the scope of EU law. The feeling that "double standards" are prevailing, and that the EU is intruding, for reasons that can barely be justified, on key US national security activities, haunts US government officials.

Four problems with the US position

The US arguments sound powerful and coherent. There are, nevertheless, at least four problems with these arguments.

1) Failure to take into consideration the ECHR dimension

As we have seen, the US submissions are based on the argument that "EU Member State direct access measures are not subject to EU law at all" and "a data exporter would have no comparative standard by which to assess whether privacy protections offered by a destination country for the same type of activities are "essentially equivalent" to protections required by EU law". (here at 9 or here at 7)

While this is true in relation to "EU law" *stricto sensu* (due to the scope of national security exceptions in EU data protection law), this reasoning neglects the fact that the European Convention on Human Rights (ECHR) and its Article 8 on privacy (amongst others) are applicable to surveillance laws. Of course, the ECHR is not binding in EU law as the EU has not acceded to it. However, the ECHR is binding upon **all** EU Member States and forms part of European law *lato sensu*.

Consequently, principles such as legality (the need for a clear legal basis for meeting certain quality requirements); necessity and proportionality; independent oversight; and effective remedies/redress etc. **do** govern EU Member States' surveillance laws. The European Court of Human Rights (ECtHR) has issued a great number of surveillance judgments, and the issue of whether methods used by governments constitute

"direct" or "indirect" surveillance (in terms of requests to service providers) seems of little relevance to the underlying principles concerning protection.

In his Opinion in *Schrems II*, Advocate General Saugmandsgaard ØE stressed that "the provisions of the ECHR will constitute the relevant reference framework for the purpose of evaluating whether the limitations that the implementation of EO 12333 might entail — in that it authorises the intelligence authorities to collect personal data themselves, without the assistance of private operators — call into question the adequacy of the level of protection afforded in the United States" (§ 229).

The importance of this ECHR dimension is also shown by the reference to ECtHR case law in the November 10, 2020 EDPB "Recommendations on the European Essential Guarantees for Surveillance Measures" (EDPB EEG Recommendations). In a similar way, the draft GDPR decision on UK adequacy published by the European Commission heavily emphasises the fact that the UK has ratified the ECHR and that "all public authorities in the UK are required to act in compliance with the Convention" (§ 116).

2) Old wine in new bottles?

While US arguments are presented in these two submissions for the first time in such specific way, in reality similar arguments have already been put forward by the US Government in the past and have been rejected by both the EDPB (see for instance § 86 of the Second Annual Joint Review of the Privacy Shield, 22 January 2019) and the CJEU. During the *Schrems II* proceedings, for instance, the argument that the adequacy assessment should not include EO 12333 was put forward both by the US government and Facebook. The Court did not uphold it, however, and referred to EO 12333 multiple times (17 times in total!) making no distinction between this Executive Order and FISA 702 in terms of assessing the "essential equivalence" of US surveillance law.

This indicates that, if EO 12333 is excluded from the scope of the Privacy Shield's successor, it will **highly increase** the risks of it being invalidated again by the CJEU in a future "Schrems III" case.

3) Teleological Interpretation

One of the most important objections to the US arguments must be based on a teleological interpretation of Chapter V of the GDPR (on transfers of personal data to third countries or international organisations). The entire logic of the GDPR is that European personal data should travel with protection. If European data can be intercepted legally by the US Government while transiting from Europe to the US without any application of European surveillance safeguards, then there is no protection. What is the point of introducing safeguards once the data have already been transmitted to the US (in accordance with FISA 702 and "indirect access"), if bulk interception of the same data can take place with no European equivalent protection, by accessing the transatlantic cables? It is logical, then, that the protective mechanism of Chapter V would either mean that the data is not transferred at all or that robust encryption is used in order to protect the data during the transit. As

the Advocate General stressed in his *Schrems II* Opinion, the requirement, set out in Article 44 of the GDPR, that there be continuity with regard to the level of protection, means that the level must be adequate throughout the transfer, including when the data travel via submarine cables to the US.

4) Responding to the "punishing the virtuous governments" argument

In his *Schrems II* Opinion, the Advocate General also responded to the above (persuasive) US argument about the fact that transparent and virtuous governments could be "punished" by the EU approach, in the following way:

> "The fact that it is impossible, as Facebook Ireland and the United States and United Kingdom Governments submit, to ensure that another third State will not secretly collect those data while they are in transit, does not affect that evaluation. Moreover, such a risk cannot be precluded even after the data have arrived on the territory of the third State of destination.
>
> It is also true, moreover, that when the Commission assesses the adequacy of the level of protection guaranteed by a third country it might find that that third country fails to disclose to it the existence of certain secret surveillance programmes. It does not follow, however, that, *when such programmes are brought to its knowledge*, the Commission may refrain from taking them into account in its examination of adequacy. Likewise, if, after the adoption of an adequacy decision, the existence of certain secret surveillance programmes, implemented by the third country in question on its territory or while the data are in transit to that territory, is disclosed to it, the Commission is required to reconsider its finding as to the adequacy of the level of protection ensured by that third country if such disclosure gives rise to doubt in that respect." (§§ 237 and 238, original emphasis).

As a conclusion to this first part, there are powerful arguments that the EU could use in order to counter the US position according to which direct/non-compulsory access to data by US intelligence agencies should be excluded from the scope of EU/US adequacy negotiations. However, as we will see in Part 2 of this article, the US could reasonably oppose an equally strong and legitimate number of counter-arguments – which raises the question of how the two sides could get out of this mess.

The second part of this article will be published here tomorrow morning.

Footnotes

1. EO 12333 is one of the two major US surveillance authorities discussed in Schrems II. I present EO 12333 more in detail later in this paper. ↩
2. "EO 12333 authorizes no compulsory access so there can be no "requirement" on the basis of EO 12333 alone for a company to disclose any data to the U.S. government" (here at 8). ↩

3. EO 12333 was first issued by President Reagan in 1981 and last amended by President Bush in 2008. It does not authorize any specific intelligence-gathering program but establishes goals of US intelligence, assigns roles and responsibilities to the entities that comprise the US intelligence community and provides a general framework for surveillance and a number of limits that must be respected by all procedures giving specific powers to intelligence agencies to conduct surveillance under EO 12333. ↩

4. Section 2.4 of EO 12333 provides nonetheless for an exception giving to the FBI the possibility to undertake "unconsented physical searches" or electronic surveillance of a US person *within* the territory of the US. My understanding is that this relates to typical law enforcement activities that would be subject to typical limitations (a warrant with probable clause, etc.) ↩

5. For access to underseas cables by French intelligence agencies see for instance here and here. ↩