European Law Blog

Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy Negotiations (Part 2)

Theodore Christakis

European Law Blog

Published on: Apr 13, 2021

DOI: https://doi.org/10.21428/9885764c.48a614b8

Part 2: On Double Standards and the Way Forward

In **Part 1** of this article, published yesterday here, I explained how the US government tries to exclude Executive Order 12333 and international surveillance from the scope of the EU/US adequacy negotiations and I presented four possible responses to the US arguments. In this second Part, 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 to get out of this mess without endangering the continuity of protection of EU personal data required by the GDPR.

It is not clear whether the ECHR is really applicable to international surveillance

As discussed in Part 1, the US argues that direct or non-compulsory access to data should be excluded from the scope of EU-US adequacy negotiations because "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". I argued that this statement, formulated in such broad terms, seems to be wrong, because the ECHR is binding upon all EU Member States and thus offers such a "comparative standard" in relation with direct or non-compulsory access. However, the point that I will make here is that such a "comparative standard" only exists in relation with *domestic* surveillance activities of European States. The assumption that the ECHR is applicable in a situation in which *international* surveillance is being conducted, is far from what you would call an axiom.

Claiming that the ECHR applies to surveillance activities undertaken *outside* the territory of the state parties, raises the crucial question of whether the ECHR has extraterritorial application. Article 1 of the ECHR lays down the principle that "[t]he High Contracting Parties shall secure to everyone *within their jurisdiction* the rights and freedoms defined in Section I of this Convention" (emphasis added). In its case law the ECtHR has stressed that the critical test to determine whether the ECHR has extraterritorial application is that of "effective control", which can be exercised by a State party in the territory under consideration. In the famous *Loizidou v. Turkey* judgment of 1995, for instance, the Court held Turkey accountable for violations of the Convention that took place outside Turkey's territory on the basis that these violations were the "result of the continued occupation and control of the northern part of Cyprus by Turkish armed forces".

Yet in another landmark judgment, *Bankovic and Others v. Belgium and 16 Other Contracting States* (2001), which concerned the bombing of Serbia by NATO European forces during the Kosovo crisis, the Court refused that there was any "effective control" and held that the bombing of the applicants by State Parties did not establish "any jurisdictional link between the persons who were victims of the act complained of and the respondent States" (§ 82). The Court adopted a restrictive view on jurisdiction and emphasized that "the

Convention was not designed to be applied throughout the world, even in respect of the conduct of Contracting States" (§ 80). Although *Bankovic* has been somehow rendered more nuanced by subsequent judgments, the Court has preserved its basic outcome and the conceptual basis for it. If in the future the Court applies *Bankovic's* restrictive approach on jurisdiction to extraterritorial surveillance, then it might well declare the ECHR inapplicable.[1] As Marko Milanovic wrote: "following the logic of Bankovic, if dropping a bomb on someone does not suffice to create a jurisdictional link extraterritorially, then reading their emails or the hacking of their phone would not suffice either".[2]

It should be emphasized that, today, there is not a single ECtHR judgment that concerns *international* surveillance, i.e. interceptions that take place *outside* the territory of a state party.

Scholars sometimes refer to the *Liberty and Others v. the United Kingdom* (2008) case, due to the fact that it concerned two Irish NGOs neither of which was physically present in the territory of the UK. However, in this case the two Irish NGOs had communicated with a third, British NGO, and their communication was allegedly intercepted in the UK by British authorities. The UK government did not raise any issue with respect to jurisdiction under Article 1, which is also illustrative of the fact that this case was not about the extraterritorial application of the Convention.

The *Centrum för Rättvisa v. Sweden* judgment of June 19, 2018 could represent a better candidate in the sense that the applicants challenged strategic foreign surveillance powers under Swedish law, which does not permit the interception of communications within Sweden. However, here as well, the bulk interception of electronic signals took place in a State Party to the ECHR, namely Sweden, and concerned signals that cross the Swedish border in cables owned by a communications service provider.

The *Big Brother Watch and Others* 2018 judgment was the first ever case concerning "intelligence sharing". However, here again, it is hard to claim that this case concerned "international surveillance". As the Court stated: "nor did [the applicants] suggest that the interception of communications under the section 8(4) regime was taking place outside the United Kingdom's territorial jurisdiction. The Court will therefore proceed on the assumption that the matters complained of fall within the jurisdictional competence of the United Kingdom." (§ 271).[3]

In fact, the only judgment that has been issued in Europe that concerns international surveillance occurred in a domestic court. On May 19, 2020 the German Federal Constitutional Court held that German intelligence services, in conducting extraterritorial surveillance activity, must respect the privacy guarantees set out in the German Grundgesetz (i.e. the Constitution) even when their operations only involve foreigners in a foreign country (so-called "foreign-foreigner" espionage). Observers noted that this decision "advanced a revolutionary vision of the state's ancient prerogative to pursue foreign espionage", while NGOs welcomed what they called a "landmark decision", a "ruling [that] sends an international signal and could affect the surveillance activities of other countries' intelligence services". However, the German Constitutional Court

solely based its conclusions on German constitutional law. It noted that under the ECHR there "has been no final determination as to whether protection is afforded against surveillance measures carried out by Contracting Parties in other states" (§ 97) and added that the ECHR "does not stand in the way of the applicability of German fundamental rights abroad" (§ 99).

Even if the ECHR is applicable, does it impose tough and authentic limitations to international surveillance laws?

Even if the ECHR was applicable, this would not mean that there will be no double standards in relation to what the EU seems to be requesting from the US and the real limitations that the ECHR imposes on European international surveillance laws.

First, even if the ECHR was theoretically applicable, it is far from clear what the applicable standards for international surveillance laws would be. Under the doctrine of the "national margin of appreciation", the ECtHR has a long history of deference to the pressing national security needs of European States, although these are balanced with the importance of the interference to the rights guaranteed by the convention. If national security considerations (and the specific exceptions introduced in Article 4(2) of the Treaty on European Union and secondary EU law) are powerful enough to exclude direct access by intelligence agencies from the scope of EU law, then the ECtHR might, similarly, consider that a very wide national "margin of appreciation" should be granted to the ECHR's state parties when it comes to international surveillance.

Second, the assumption that because EU Member States are parties to the ECHR their international surveillance laws automatically comply with the Convention's (hypothetical) standards is simply wrong for the following reasons:

- The ECtHR has emphasized that although a state may be a party to an international Human Rights Treaty, this does not necessarily mean that this State will respect this treaty. In *Saadi v. Italy* (2008) for instance, the Court stressed that "accession to international treaties guaranteeing respect for fundamental rights in principle are not in themselves sufficient to ensure adequate protection…" (§ 147). It may well follow then that the international surveillance laws of the vast majority of EU Member States *do not* meet ECtHR standards (this may be the case, for instance, with French international surveillance law, as we will see in the next Subsection).
- In any case, this is something that we may never learn about or only learn about after waiting for several years. International surveillance laws are rarely, if ever, challenged before the ECtHR. All of the 14 pending challenges against the current French surveillance system, for instance, solely target the July 24, 2015 Intelligence Act on domestic surveillance. To my knowledge (see here and here), none of them targets the November 30, 2015 French Act relating to measures for the surveillance of international electronic communications.

- Even in the theoretical scenario where an international surveillance law of a European state is challenged, it often takes several years for the ECtHR to issue a judgment, allowing the intelligence agency in question to function unhindered during this period. For instance, challenges to the French Intelligence Act of 24 July 2015 are still pending before the ECtHR (see links in previous paragraph), six years after their filing.
- Finally, when the ECtHR finally publishes its judgments, it is far from clear whether European states will comply with them. The problem of State Parties' compliance with ECtHR judgments is a serious and notorious one. George Strafford noted that, despite efforts by the Council of Europe to minimize it using a positive "narrative" and "rosy" statistics, the problem is so important that it could be compared to a "hole in the roof" of ECtHR's palace. Execution of the ECtHR judgments concerning surveillance could represent a particularly difficult problem. The latest "Table of cases and groups of cases under enhanced supervision" published by the Committee of Ministers of the Council of Europe (March 15, 2021) shows that several famous surveillance judgments of the ECtHR, such as *Zakharov v. Russia* (2015) or *Szabo and Vissy v. Hungary* (2016), are still encountering problems with regard to execution, several years after the judgments. Hungary, for instance, which is an EU Member State, informed the Committee of Ministers in January 2021 (five years after the ECtHR judgment became final!) that the "examination of the requirements stemming from the judgment in terms of legislative amendments, which is currently underway, is expected to take some time".

Double Standards? Let's talk about the French International Surveillance Act

A comparison between what the EU seems to be requiring from the US and the reality of the French international surveillance Act of November 2015 (to cite just one example) could inflame US accusations of "double standards". Let's do a comparison.

The document that seems to "set the standards" for the US, at this stage, is the EDPB EEG Recommendations. As I have explained elsewhere, these Recommendations set the bar for surveillance laws very high. They "pick and choose" the strictest requirements found in the jurisprudence of the CJEU and the ECtHR without making any clear distinction between the two legal orders and without making *any* distinction between domestic surveillance and international surveillance. As a result, the impression remains that the "essential equivalence" of all US surveillance laws (including EO 12333) should be assessed against this very demanding fusion of standards. (see § 52 of the EDPB EEG Recommendations)

Now, a comparison between these EDPB standards and the November 30, 2015 French Act relating to measures for the surveillance of international electronic communications, gives the impression that the French law quite possibly does not meet these standards.

- The French Act authorises international surveillance in a very broad way and for far-reaching purposes, including, for instance, that of serving the "major interests of French foreign policy" or the "major economic, industrial and scientific interests of France" (see here).

- It authorises bulk automated surveillance for these broad purposes as well as subsequent targeted surveillance.
- It is not subject to any prior authorisation by a court or an independent administrative authority. The relevant body, the National Commission for the Control of Intelligence Techniques (CNCTR) only receives *communication* about surveillance measures taken, but does not have any *ex ante* power of control.
- While the Act provides for an *a posteriori* oversight mechanism by the CNCTR, it seems rather weak. The CNCTR cannot inform people as to whether they have been under surveillance or not – it can only inform them if an irregularity has been committed, which would be somewhat rare when you take into consideration the broad powers given to intelligence agencies under this law. Furthermore, even if the CNCTR finds that an irregularity has taken place, it cannot "block" the surveillance measures but it can make a recommendation to the French Prime Minister and, if the Prime Minister does not agree to take action, it can bring the case to the highest French administrative court. To the best of my knowledge, this has not yet happened where international surveillance law is concerned.

A situation where the EU requests that the US complies immediately with all the "European Essential Guarantees for surveillance measures" (as they appear in the EDPB EEG Recommendations), when EU Member State's international surveillance laws do not seem to meet these same safeguards, could only reinforce the US feeling of "double standards" and could hinder the fruitful conclusion of the EU-US negotiations which is absolutely essential for the continuation of transatlantic data transfers. The big question is then how the EU and the US could reach a balanced approach that takes into consideration the legitimate and fundamental interests of both sides.

Conclusion: Squaring the circle or practical solutions?

In its *Schrems II* judgment the CJEU made no distinction between domestic and international surveillance. Similarly, the EDPB in its EEG Recommendations made no distinction between the standards that should apply to domestic surveillance laws and those that should apply to their international counterparts. This leaves the impression that what is expected from the US is to "essentially" comply with all the safeguards that appear in the EDPB EEG Recommendations. If one takes into consideration that existing European laws on international surveillance do not seem to meet these standards, this could create legitimate frustration and protests of "double standards" from the US.

Of course, one could try to avoid the impression of "double standards" by using the "ECHR" card. Contrary to the CJEU and the EDPB, the Advocate General in *Schrems II* adopted a much more refined position claiming that "since the Member States' adherence to the ECHR requires that they ensure that their internal law is consistent with the provisions of that Convention", the ECHR safeguards should be the only ones used "as the relevant comparator" for the purpose of assessing whether EO 12333 offers protections that are "essentially equivalent" to those that exist in Europe.

However, as this paper has established, it is far from clear whether the ECHR applies to extraterritorial international surveillance. Even if it applied, the exact limitations that the ECHR will impose on "direct" international surveillance activities are not at all evident. Even if important limitations are imposed, it is uncertain whether the ECtHR will ever be given the opportunity to enforce such limitations. Even if the ECtHR has the opportunity in the future to criticise international surveillance laws of European countries, it is not at all certain that these countries will comply with the ECtHR judgment.

This leads us to a surprising and rather extraordinary situation which is ripe with contradictions:

- EU Member States are bound by the EU constitutive treaties, but their international surveillance laws escape the scrutiny of the CJEU as this issue falls outside of the scope of EU law. The US, in contrast, is not party to the EU constitutive treaties, but its international surveillance laws will remain forever "wedded" to the particularly demanding control of the CJEU in Schrems-like cases.
- The EU has declined for decades to become a party to the ECHR, due, mostly, to the hostility of the CJEU to this idea. The result is that the ECHR is not part of the EU legal order. Nevertheless, the EU and the CJEU are using the full force of the ECHR against the US, through the indirect, adequacy-related methods explained in this paper.
- EU Member States are parties to the ECHR, but in practice they are able to adopt far-reaching international surveillance laws with few limitations and safeguards, no prior authorisation mechanism and somewhat limited *a posteriori* The US, in contrast, is not party to the ECHR, but is required to fully and immediately comply with all ECHR (hypothetical) standards.

Of course, nothing prohibits the EU from trying to take advantage of this complex situation in order to impose limitations on the US that do not currently apply *de facto* to EU Member States. After all, the EU could argue that only EU Member States benefit from the national security exemption of TEU Article 4(2); that the peculiar distinction drawn in the *LQDN* judgment between indirect/compulsory and direct/non-compulsory interception is only understandable as an effort to give some meaning to the Article 4(2) exemption; and that the US, not a member of the EU, is not eligible to take advantage of that distinction. In other terms the EU could plainly "assume" the "double standards" doctrine and try to press the US to change the way its intelligence community exercises "the second oldest profession" at the international level – without being able to do so domestically for European intelligence agencies.

However, this might create legitimate strong reactions by the US side and might not be the best way to build the ambitious new transatlantic agenda sought by the EU. One could argue that transatlantic relations would be better served by a balanced approach, based on friendly historical ties, trust, mutual respect and reciprocity. Indeed, the idea that any agreement between the EU and the US "should create reciprocal rights and obligations of the parties" is an essential condition set by the Council of the EU in its mandate given to the Commission in 2019 to engage on another set of ongoing transatlantic negotiations on cross border data issues, namely the conclusion of an EU-US international agreement on law enforcement access to data. In a similar

way, the Advocate General stressed in his *Schrems II* Opinion that, in relation with surveillance issues and essential equivalence, "it would be wholly unjustified … if a third country were expected to comply with requirements that did not correspond to obligations borne by the Member States" (§ 204).

The big challenge is to try to imagine how the two sides could get out of this mess.

A first step could be to determine precisely which standards should apply. The two sides should determine whether the ECHR applies extraterritorially in relation to international surveillance activities. If this is not the case, then EO 12333 should be excluded from the scope of adequacy negotiations and the EU should recommend that robust encryption be used in order to protect the European personal data during the transit. If, nonetheless, the ECHR applies extraterritorially, then the two sides need to determine what exactly are the applicable standards and safeguards.

A second step could be to consider a new paradigm. Instead of "pushing" the US to adopt general structural changes to EO 12333, an idea that could be strongly resisted by the US intelligence community as it affects national security ("rewriting of 12333 would only be over the dead bodies of numerous senior people in the US intelligence community", told me a US colleague), the negotiations should focus on how to address the specific EU concerns. One place to start might be codifying PPD-28 (i.e. changing it into a statute[4]), while providing necessary clarifications in terms of its oversight and control.[5] More importantly, each side should clearly determine what it *needs* as opposed to what it simply *guesses* it should be done on the basis of the Schrems II judgment.

For the EU, the "need" should be to ensure that European personal data are *always* protected, wherever they are, in Europe, the US or in transit somewhere in the middle of the Atlantic. It is interesting to note in this respect that, in terms of the Privacy Shield decision, the Commission was not in a position to determine whether the United States does actually intercept communications transmitted via transatlantic cables, since US authorities did not confirm nor deny that proposition (see recital 75 of that decision and letter of 22 February 2016 from Mr Robert Litt, in Annex VI, paragraph I(a)). This time it would probably be hard to duck the question. The issue should be discussed and the two sides could consider two possible solutions in order to address the EU data protection concerns without making unreasonable demands to the US side.

First, the two sides should consider whether the use of robust encryption might be enough to secure European personal data as they transit the submarine cables and, more generally, as they are carried over optical waves across fiber-optic cables. The Snowden slides on the US intelligence community practices, including interception of underseas cables, made a deep impression on EU officials and the activist community. The legacy of the outrage lives on despite the fact that today, as I am told by ICT experts, all major providers systematically use encryption for data in transit (*anytime* that data moves) and even when data are at rest on a server. While interception of data in transit over ocean cables was an important risk previously, when most of data was transmitted in the clear, I am told that today it is pretty unheard of for data to be transmitted in the

clear - which seems to indicate that undersea cable interception in the age of widespread use of transit encryption is no longer a significant risk. As shown by all recent major cyberattacks (including SolarWinds), in the vast majority of cases[6] an attacker will attack a user's end-points directly and attempt to compromise the user's own access mechanisms through phishing or other attacks designed to compromise the user's credentials and log into their resources. The NSA could theoretically do so (and also carry out other attacks) in the territory of EU Member States on the basis of the EO 12333 framework but this has nothing to do with "data transfers" under Chapter V of the GDPR and falls clearly out of the scope of adequacy negotiations.[7] If the EU and the US wish to discuss how they spy on each other's territories this is an interesting but separate issue for the transatlantic agenda. The only "international surveillance" issue relevant under the GDPR is the one of interception of data while in transit. Intelligence agencies of course are not going to advertise what the current state of the art is on surveillance and whether the NSA has the technical capabilities to decipher and read encrypted European data, but the EU and ENISA must have the necessary expertise to assess whether robust transit encryption is an adequate response to these concerns.

Alternatively, a mutually agreed solution could occur in order to ensure that any eventual data gathering in transit that takes place in the future is accompanied by sufficient safeguards to satisfy the EU data protection requirements. Such a solution would only apply to US-EU relations and would not require from the US to change in a general way EO 12333 or affect the powers of the two sides' intelligence agencies in relation to third States.

In order to achieve such a "surgical solution", the EU and the US might have a strong incentive to start thinking about this issue through the prism of international law. The post-*Schrems II* deadlock shows that it is high time democracies actively search for common ground on surveillance standards. At the multilateral level, the ongoing process between like-minded countries at the Organisation for Economic Co-operation and Development (OECD) is welcome, although I doubt that OECD countries will dare go as far as international espionage. At the much more pressing transatlantic level, there is a great variety of international law tools that could be used, ranging from the conclusion of an EU-US agreement to much more flexible tools such as binding unilateral declarations and diplomatic assurances. These legal acts could also be combined, if needed, with commonly agreed oversight mechanisms, for instance requiring security clearances for representatives of the other side. Such tools could help the two parties find pragmatic, tailored and flexible solutions to these extremely complex issues without having to square the adequacy circle or affect their capacity to conduct intelligence activities against third countries.

Footnotes

1. In the *Big Brother Watch* case, the International Commission of Jurists claimed that: "the fact that, in a mass surveillance operation, elements of the interference with rights might take place outside a State's territorial jurisdiction didn't preclude that State's responsibility, since its control over the information was sufficient to establish jurisdiction" (ECtHR, First Section, Judgment of September 13, 2018, § 299). It is

questionable if such a position is compatible with the *Bankovic* approach where, after all, the respondent States also had complete control over the operations. ↩

2. It should be noted, however, that Milanovic is critical of the *Bankovic*'s logic. ↩

3. It should be recalled that both cases were referred to the Grand Chamber and are still pending. ↩

4. PPD-28 is currently an executive act subject to change without legislative involvement. ↩

5. For the oversight mechanisms related to EO 12333 see the Report released on April 2, 2021 by the US Privacy and Civil Liberties Oversight Board (PCLOB). While this report highlights (at p.23) that other authorities (including the Congress) can "oversee EO 12333 activities to ensure consistency with law, regulation, and, increasingly, policy considerations relating to privacy and civil liberties" it is hard to understand whether and how exactly such a control takes place in an independent and systematic way (in order, for instance, to check whether the intelligence community complies with PPD-28). The PCLOB members seem to indicate, in any case, that they are not in a position to do so when they note that, after six full years of reviewing EO 12333, "unfortunately it proved difficult and impractical for the Board to address the full framework of counterterrorism activities governed by EO 12333" and that the "Board is a relatively small agency with limited resources". ↩

6. It is theoretically possible for a sophisticated nation-state actor to engage in an attack on the provider's backend systems, but it is an extraordinarily difficult attack vector. ↩

7. One should not forget that in such a case it is up to each EU Member State to exercise due diligence, take all necessary cybersecurity measures on its territory and exercise its territorial jurisdiction in order, for instance, to prosecute (including through the use of European and international investigations and arrest warrants) any hostile actor who committed a cybercrime by violating the integrity of IT systems. ↩