



## UvA-DARE (Digital Academic Repository)

### Schrems II and Surveillance

*Third Countries' National Security Powers in the Purview of EU Law*

Irion, K.

**DOI**

[10.21428/9885764c.94e9b5d0](https://doi.org/10.21428/9885764c.94e9b5d0)

**Publication date**

2020

**Document Version**

Final published version

**License**

CC BY-SA

[Link to publication](#)

**Citation for published version (APA):**

Irion, K. (2020). Schrems II and Surveillance: Third Countries' National Security Powers in the Purview of EU Law. Web publication or website, European Law Blog. <https://doi.org/10.21428/9885764c.94e9b5d0>

**General rights**

It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

**Disclaimer/Complaints regulations**

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: <https://uba.uva.nl/en/contact>, or a letter to: Library of the University of Amsterdam, Secretariat, P.O. Box 19185, 1000 GD Amsterdam, The Netherlands. You will be contacted as soon as possible.

**European Law Blog**

# **Schrems II and Surveillance: Third Countries' National Security Powers in the Purview of EU Law**

**Kristina Irion**

**European Law Blog**

**Published on:** Jul 24, 2020

**URL:** <https://europeanlawblog.pubpub.org/pub/schrems-ii-and-surveillance-third-countries-national-security-powers-in-the-purview-of-eu-law>

**License:** [Creative Commons Attribution-ShareAlike 4.0 International License \(CC-BY-SA 4.0\)](https://creativecommons.org/licenses/by-sa/4.0/)

On 16 July 2020 the Court of Justice of the European Union (CJEU) composed as Grand Chamber delivered its landmark ruling *Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems* (case [C-311/18](#), “*Schrems II*”). For the background and a discussion of the implications of the ruling for commercial transfers of personal data see the commentaries by [Christopher Kuner](#) and [Theodore Christakis](#). The focus of my commentary will be on the aspect that EU law on cross-border transfers of personal data to a third country is not deferential to national security powers of that third country. This judgment is remarkable provided that electronic surveillance conducted by Member States’ intelligence authorities for the purpose of [national security is off limits for EU law](#) and that [exceptions in international agreement](#) are fairly regularly made for national security. This contribution will deal with the embedded assessment of a third country’s national security powers under the General Data Protection Regulation (Regulation (EU) [2016/679](#), GDPR) and will address the [criticism](#) that a third country is held to stricter standards than a Member State of the Union.

*Schrems II* is a continuation of the CJEU’s 2015 judgment in *Maximilian Schrems v. Data Protection Commissioner* ([Case C-362/14](#), “*Schrems I*”), which invalidated the Commission’s Decision approving the EU-US Safe Harbour agreement (Decision 2000/520). The ruling notes that the Safe Harbour Decision carries a provision that “national security, public interest, or law enforcement requirements” have primacy over the Safe Harbour principles (para. 86). However, any interference with the rights to privacy and the protection of personal data as guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights in the European Union (Charter) must be limited to what is strictly necessary and the right to effective judicial protection must be observed (paras. 92-95).

### **Consideration of a third country’s national security legislation**

In the *Schrems II* ruling the Court held that not only an adequacy decision by the Commission but also the use of Standard Contractual Clauses (SCCs) require a level of protection in a third country that is essentially equivalent to that guaranteed within the EU (paras. 104, 137). The Court interprets Article 46(1) and (2)(c) in connection with Article 45(2) of the GDPR to the effect that economic operators when they transfer personal data on the basis of the SCCs must take into consideration the relevant aspects of the legal system of that third country, including national security, as regards any access by public authorities of that third country to the personal data transferred (para. 105). SCCs form by their nature a contract under private law between economic operators which implies that SCCs “are not capable of binding the authorities of that third country” (para. 125). The validity of the Commission Decision [2010/87/EU](#) (SCCs Decision) was however not affected (para. 148) because the burden to verify that the recipient of the personal data in the country of destination can honour the level of protection required by EU law is placed on the economic operators which make use of SCCs and is subject to the supervision by the competent data protection authority of an EU Member State (paras. 135, 137, 142 and 146).

### **Interferences from US Surveillance Programmes are not limited to what is strictly necessary**

In order to neutralize a perceived legality flowing from Decision (EU) [2016/1250](#) of the Commission on the adequacy of the protection provided by the EU-US Privacy Shield (Privacy Shield Decision) the Court entered into an analysis of that decision paying special attention to US surveillance powers. The Court held that Section 702 of the US Foreign Intelligence Surveillance Act (FISA) “cannot ensure a level of protection essentially equivalent to that guaranteed by the Charter” for the reasons that this Section “does not indicate any limitations on the power it confers to implement surveillance programmes for the purpose of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programmes” (para. 180). The Court also dismisses US Executive Order (E.O.) 12333 which authorizes access to data in transit to the US without that access being subject to judicial review as failing to “delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data” (para. 183). Furthermore, being an oversight mechanism inside US law, Presidential Policy Directive 28 (PPD-28) “does not grant data subjects actionable rights before the courts against the US authorities” (para. 181). Finally, also the Ombudsperson Mechanism that forms part of the Privacy Shield Decision is deficient and lacking substantive guarantees of “the Ombudsman’s independence from the US executive”(para. 195) and the Ombudsman has no “power to adopt decisions that are binding on intelligence services” (para. 196). The CJEU concludes that interferences arising from these US surveillance programmes are not limited to what is strictly necessary and that EU data subjects whose data have been transferred have no recourse to effective administrative and judicial redress (paras. 180f.). Hence, the Commission’s finding of an adequate level of protection provided by the EU-US Privacy Shield is not tenable and the Court invalidated the Privacy Shield Decision without temporal restrictions.

### **Economic operators are liable to ensure essentially equivalent protection**

It is evident that cross-border transfers of personal data sourced from individuals in the EU to a commercial operator based in a third country are intertwined with the destination country’s legal system, including the often secrecy-cloaked practices of national intelligence. The *Schrems II* ruling clarifies that the possibility that personal data of EU data subjects which are transferred to a third country as part of a commercial transaction “might undergo, at the time of the transfer or thereafter, processing for the purposes of public security, defence and State security by the authorities of that third country cannot remove that transfer from the scope of the GDPR” (para. 86). The finding summarily rejects several objections raised against the application of the GDPR to the transfer of personal data for commercial purposes by an economic operator established in the Union if the data that have been transferred are liable to be processed by the authorities of that third country.

First, Article 4(2) TEU which provides that “national security remains the sole responsibility of each Member State”, thereby carving out national security competences from the scope of EU law, concerns only Member States of the Union (para. 81). Second, the possibility that personal data transferred between two economic operators could be accessed by the authorities of the third country for the purposes of public security, defense and state security does not exclude the transfer from the scope of the GDPR pursuant to Article 2(2) GDPR

(para. 85). In the event of a transfer of personal data for commercial purposes to a third country, neither can the economic operators involved relegate their responsibility to ensure a level of protection essentially equivalent to that which is guaranteed within the EU, nor are activities by public authorities of that third country in the field of national security excluded from the scope of EU law or the GDPR.

### **Charter-based fundamental rights test applied to a third country's legal system**

The judgment is emblematic of the formal strength of the EU's fundamental rights approach to personal data protection but also its limits in the [age of digital interdependency](#). As argued in a co-authored publication [elsewhere](#), the legal architecture of the right to the protection of personal data is a solid one, with two strong constitutional pillars accompanied by an extensive legislative framework (the Charter-Treaty-Regulation triptych). The Court not only consistently interprets the GDPR in light of the Charter, but moreover uses its precedent on an EU data retention measure (e.g. *Digital Rights Ireland and Seitlinger and Others*, Joined Cases [C-293/12 and C-594/12](#)) to define the constitutional contours of an adequate level of protection relevant also in relation to a third country (paras. 170f). As a result, in order to qualify for an adequacy finding, a third country's legal system is assessed following a classical fundamental rights test requiring that an interference with Articles 7 and 8 of the Charter must be provided for by law and limited to what is strictly necessary as provided for by Article 52(1) of the Charter as well as ensuring effective judicial protection for EU data subjects corresponding with Article 47 of the Charter (para. 174f., 178, 186f.). While the ruling upholds the [GDPR's rule export to non-EU countries](#) it will also make it much harder for third countries to qualify for an adequacy finding by the Commission, and perhaps undermine the ability to mainstream adequacy decisions for the transnational governance of personal data flows.

### **GDPR limitations on transfers of personal data in relation to a third country's national security**

The *Schrems II* ruling is unprecedented for the level of detail with which the CJEU interrogates the most controversial aspects of the Privacy Shield Decision that concern US bulk surveillance programmes, including PRISM and UPSTREAM, that have been notorious since the 2013 [media coverage](#) of Edward Snowden's revelations. It is however important to bear in mind that these details are subject to the proceedings by virtue of the Privacy Shield Decision of the Commission. As a matter of fact the Privacy Shield Decision provides much more detail in relation to US law on national security and surveillance, as compared to its predecessor, the Safe Harbour Decision. Invalidating the Privacy Shield Decision, therefore, is much less a "sanction" for the existence of US surveillance programmes than it is a corrective measures against executive overreach by the Commission which again underwrote an adequacy finding for commercial transfers of personal data to the US even though the conditions from the *Schrems I* ruling have not been met.

### **EU Member States' national security is off limits for EU law**

What can be puzzling for observers of such principled CJEU jurisprudence are the [different paths](#) that the legal argument takes depending on whether an EU Member State or a third country conducts electronic surveillance for the purpose of national security. Several EU Member States, among which Germany, France, the Netherlands, Sweden and UK, are to varying degrees [implicated in electronic surveillance](#). The reception of the *Schrems I* and *II* rulings can have a flavor of differential treatment afforded to a third country as compared to an EU Member State, even though the divisive rationale of Article 4(2)TEU is deeply engrained in the foundations of EU law. The consequence of falling outside the scope of EU law is that the CJEU has no competence to review electronic surveillance conducted by a Member State of the EU in the field of national security. However, where the Court has seized the competence of judicial review over EU and its Member States' legislation, i.e. in relation to mandatory data retention schemes for the detection, investigation, and prosecution of serious crime, the Court's proportionality assessment is consistent with that of its rulings in *Schrems I* and *II* (see *Digital Rights Ireland and Seitlinger and Others*, Joined Cases [C-293/12 and C-594/12](#); *Tele2 Sverige AB v Postoch telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, Joined Cases [C-203/15 and C-698/15](#)).

Now consider Brexit, which is the first time that a country disintegrates from the EU, and how losing EU membership will change the UK's status vis-à-vis the EU to a third country. As an EU Member State, the UK's surveillance practices for the purpose of national security have not been inside the purview of EU law and the country could freely receive and share personal data inside the digital single market. When the transition period ends on 31 December 2020, transfers of personal data from the EU to the UK will be governed by Chapter V of the GDPR. In order to receive personal data from the EU as a third country, the UK's legal system, including national security, must ensure a level of protection essentially equivalent to that guaranteed within the EU. Currently, [the Commission is in the process of assessing](#) whether the UK qualifies for a finding of an adequate level of protection pursuant to Article 45 of the GDPR, read in light of the Charter. Where before there were none, the hurdles in EU law are suddenly pretty high.

### **Standards of review of national security in European human rights law**

Nevertheless, an EU Member State's surveillance practices that are based on national security powers are accountable to domestic (constitutional) safeguards, intelligence oversight and subject to judicial review by national courts. It must be conceded that a number of European countries, in their national security powers, operate a logic quite similar to the US that differentiates between the limitations and safeguards afforded to domestic targets and those afforded to foreign targets of electronic surveillance. Such a differentiation is highly problematic, I argue [elsewhere](#) that tying in the protection of communications secrecy, privacy and personal data with citizenship or residency will expose users' electronic communications and online activities to surveillance by all other countries in relation to which an individual is a foreigner or an alien. In light of today's planetary scale computation and the need for the protection of data privacy regardless of frontiers, such a logic will, following Marko Milanovic, "[ultimately prove unstable and unpersuasive](#)".

In this context it is remarkable that the German Federal Constitutional Court, in its recent decision of 20 May 2020 (Case [1 BvR 2835/17](#)), clarified that the protection afforded by fundamental rights vis-à-vis German state authorities is not restricted to the German territory and protects foreigners in other countries, here in the context of foreign telecommunications surveillance conducted by the German Federal Intelligence Service. Giving recognition to the expanding sphere of action of German state authority in the course of internationalisation, the Court continues, must be met with accepting national human rights guarantees beyond national borders (para. I.1.). The German ruling, which is the first of its kind in Europe, marks an important revision from tying the protection of fundamental rights to German territory or citizenship to guaranteeing fundamental rights in relation to the actions of German public authorities that produce extraterritorial effects.

Besides, all Member States of the EU are members of the Council of Europe (CoE) and signatories to the European Convention on Human Rights (ECHR). Article 8 of the ECHR provides for the right to respect for private and family life, and interferences by public authorities with the exercise of this right must be in accordance with the law and necessary in a democratic society in the interests of national security, among others. Complaints against a CoE Member State's surveillance practices for the purpose of national security can be lodged at the European Court of Human Rights (ECtHR). The [ECtHR case-law on national security](#) provides for a margin of discretion for national authorities but insists on the quality of the law on which the strategic surveillance is based, which must be accessible to the person concerned and have foreseeable consequences. At present, the standard of judicial review by the ECtHR over a Member State's surveillance for national security purposes is not as strict as the requirements stemming from the GDPR for commercial transfers of personal data to a third country as regards access to the data transferred by national authorities of that country. In contrast to EU law requiring surveillance to be limited to what is strictly necessary, the ECtHR recently confirmed its deference to bulk interception regimes in the service of national security which is left to a Member State's margin of appreciation (see e.g. Case *Big Brother Watch v. United Kingdom*, Applications nos. [58170/13](#), [62322/14](#) and [24960/15](#), para. 314). Soon, the ECtHR Grand Chamber will have the opportunity to revisit its case law concerning the surveillance of electronic communications in the cases *Big Brother Watch v. United Kingdom* and *Centrum för Rättvisa v. Sweden* (Application no. [35252/08](#)). Note, however, that the surveillance cases of the ECtHR directly concern the compatibility of a CoE Member State's electronic surveillance for national security with Article 8 of the ECHR, which differs from the situation of the GDPR.

## Conclusions

*Schrems II* is a good decision for the protection of EU data subjects against national security excesses of third countries that feast on international data flows. Economic rationales underpinning international data flows can be reconciled with fundamental rights. The German ruling accommodating the extraterritorial application of fundamental rights marks an important constitutional development in the right direction. Eventually, also the

US is considering ramping up the [protection of its citizens' data](#) against potential interferences by foreign governments, although not on grounds of data privacy but [national security](#).