Vienna, 18. 12. 2019

Prep-Document for December 19th 2019:
C-311/18 *Facebook Ireland* and *Schrems* ("Schrems II"), Advocate General Opinion

In preparation of the delivery of the non-binding advisory opinion of the Advocate General on December 19th at about 9:45 in Luxemburg, we have compiled the following preparation document. The case is pending for 6.5 years, deals with complex EU privacy and US surveillance laws and was subject to four hearings before different courts. It is therefore highly complex.

Further Information (general): Send an email to media@noyb.eu to be put on our media list. +43 660 2678622; media@noyb.eu

Further information for Ireland: Gerard Rudden, ARQ Solicitors *(representing Mr Schrems)* +353 1 661 6102; gerard.rudden@arqsolicitors.com

Further information on US law: Ashley Gorski, ACLU; media@aclu.org

Background of the case

US Surveillance. As the disclosures by Edward Snowden confirmed, many large US internet companies (in this case Facebook) fall under a duty to allow the US government to access European user data on a mass scale for "foreign intelligence" purposes (including anti-terrorism and espionage). Such use of Europeans' data may well be *against* the national interest of the EU and its member states (for example when enforcing US sanctions against EU companies or when spying on EU citizens and governments).

The 2015 "Safe Harbor" case. Based on these facts, Mr Schrems filed a complaint against Facebook with the Irish Data Protection Commissioner ("DPC") in 2013. The DPC first rejected the complaint as "*frivolous and vexatious*". Mr Schrems appealed against the DPC and ultimately won: In that case, C-362/14 *Schrems*, the CJEU ("Court of Justice of the European Union", the EU's supreme court) confirmed his view and ruled that mass surveillance violates European fundamental rights. The CJEU struck down the previous "Safe Harbor" system that facilitated EU-US data transfers. This system was urgently replaced with the "Privacy Shield" system in 2016. Schrems: "*Privacy Shield is an updated version of the illegal 'Safe Harbor'. Nothing in US surveillance law was changed or fixed*."

Standard Contractual Clauses ("SCCs"). After the first CJEU decision on "Safe Harbor", Facebook claimed it would *not* use "Privacy Shield" but so-called "Standard Contractual Clauses" (SCCs).
SCCs are a *contract* between an EU company (here Facebook Ireland) and a non-EU company (here Facebook Inc, in California) in which the foreign company pledges to respect Europeans' privacy. The law accepts that such contracts sufficiently protect European data when transferred abroad.

Core Problem: EU privacy law clashes with US surveillance law. Under the EU privacy laws ("GDPR") and the SCCs, a "*data export*" to a third country is only legal if the exporting company (in this case Facebook Ireland Ltd) can ensure *"adequate protection"* in the US. In practice, this turned out to be impossible, because US surveillance laws (such as FISA 702 and EO 12.333) result in the US

government's "*mass processing*"[1] of personal data for surveillance purposes. Schrems: "*In simple terms: EU law requires privacy, while US law requires mass surveillance. The question is, what happens when an EU company follows US rather than EU law?*"

Application of Mr Schrems & Reaction by the Irish DPC. Given the situation above and the ruling of the CJEU in the "Safe Harbor" case, Mr Schrems consequently requested the Irish DPC in 2015 to use Article 4 of the SCCs, which allows the DPC to order Facebook to "suspend" the data transfers in individual cases. While the DPC now agreed with Mr Schrems that US surveillance laws violate EU law, they did not take direct action. Schrems: "*We asked for a targeted solution, only for companies that fall under these surveillance laws. The DPC could have issued such a decision within a day*."

Irish DPC wants to invalidate SCCs. The DPC however did not follow the request of Mr Schrems, but instead filed a lawsuit against Facebook and Mr Schrems before the Irish High Court, with the aim to refer the case back to the CJEU - this time on the validity of the SCCs. The Irish High Court has complied with the DPC's request and referred eleven questions to the CJEU, despite the resistance of Mr Schrems and Facebook (who both opposed the reference for different reasons). Gerard Rudden (of ARQ Solicitors, representing Mr Schrems): "*My client asked for a targeted solution for companies that fall under US mass surveillance laws. The DPC could have issued such a decision long ago. Instead, after 7 years and two referrals to the CJEU, we still have no formal decision from the DPC.*"

***noyb.eu* & Legal Team** Mr Schrems has brought this case on a pro-bono basis and is supported by a team of lawyers from Ireland, the US and Luxembourg. The case is also supported by the European non-profit organization *noyb.eu*, of which he is also the honorary chair. Mr Schrems is represented by Eoin McCullhan, instructed by Ahern Rudden Quigley Solicitors. Prof. Herwig Hofmann supported the case on European Law matters. Ashley Gorski of the American Civil Liberties Union (ACLU.org) has assisted as an expert witness on US surveillance law.

Possible outcomes

Difference between AG opinion and final judgement very likely. The case raised eleven partly interconnected questions with many additional issues that come with each question. Unlike in many other cases there is no binary answer to be expected. The opinion and the final judgement can both expand on some issues further and stay silent on other points. Schrems: "*This case has eleven interconnected questions. It is very unlikely that we will get a single clear 'yes or no' answer from the Advocate General. Given the many options, it is even less likely that the Judges will approach these eleven questions the same way in their final judgement."*
On top of the many different options in this case, the oral hearing of the case could have been an indicator of somewhat different views between AG and the Judges. Schrems: "*During the court hearing the Advocate General asked questions in a very different direction than the Judges. The judges seemed to be much more critical of US law and the assessment by the Europeans Commission than the Advocate General. I therefore expect that the final judgment may provide stricter privacy protections than the opinion on Thursday."*

Long-term solution needed. In the long term, the fundamental clash between EU privacy laws and US surveillance laws will very likely not be resolve in this case. Schrems: "*If the US wants to process the data of foreigners, it will have to give foreigners at least the same baseline privacy protections. Right now, the US behaves a bit as if Switzerland would say 'store all your gold with us, but actually you have no rights once it is here'. If that's the situation who in the world will trust the US with his data?"*

[1] Finding by the Irish High Court (referring court)

Position of the Parties on the "Main Dispute"

Once a data protection authority is of the view that a recipient of data is under legal obligations in a third country that does not comply with EU law (as in this case), the question arises how to solve this dilemma. The three parties in the procedure proposed three different answers:

	Irish DPC	Max Schrems	Facebook
US surveillance doesn't violate EU law *("no problem to solve")*	No	No	Yes
Article 4 SCCs allows to suspend ("*targeted solution*" for FISA companies)	No	Yes	Yes, *if there would be a problem*
SCCs are invalid globally *("radical solution")*	Yes	No	No

➔ Facebook is of the view that the premise of the question is wrong, because US surveillance is compliant with EU law (for various reasons) and the case is not governed by EU law.

➔ Mr Schrems is of the view that Article 4 of the SCCs allows the DPC to suspend data flows in individual cases, but the DPC is not making any use of this "targeted solution" under the law.

Note: Most EU member states, the European Commission and even Facebook and some industry lobby groups agree that if there is a conflict with third country law, that this is the solution.

➔ The DPC sees a "systematic" problem that should lead to the invalidation of the SCCs globally and it should not be upon the DPC to act in each case individually.

Note: This view was not supported by any other party, Member State or EU institution during the hearing before the CJEU. The DPC is the only party that has taken that view.

FAQs & Common Misunderstandings

- **Didn't Mr Schrems try to take down the Standard Contractual Clauses?**

Mr Schrems has never argued that the SCCs may be invalid. Of all parties and all interventions at the CJEU only the DPC took the view that the SCCs should be invalidated. Everyone (EU institutions, Member States, Lobby Groups, Facebook and Mr Schrems) are of the view that the SCCs are not invalid.

- **Isn't the EU just blocking free trade?**

There are two laws that lead to this clash of jurisdictions: (1) US surveillance laws that allow mass surveillance of foreigners and espionage without individual court approval and (2) the European fundamental right to privacy. It is highly rational to prohibit data flows to a foreign territory, if this data may be misused. The US has similar concerns regarding apps like "TikTok" or 5G hardware by Huawei.

- **Doesn't this case mean that you cannot send emails to the US anymore?**

In simple terms, the GDPR speaks to two types of data flows: (1) Necessary data flows (like emails or booking a hotel abroad), for which there are derogations in Article 49 GDPR and (2) cases of "outsourcing" of data processing to a third country, which are not strictly necessary. Even if the SCCs would be invalidated, this would only have consequences for the second category of cases, in which no "derogation" applies.

For emails this would mean that a Gmail mailbox as a whole may not be outsourced to the US anymore, but individual emails that go to a US friend or colleague will still be delivered (just like emails are sent to China, Russia or even North Korea today).

- **Does this case concerns all data flows to the US?**

According to Mr Schrems' arguments, the core issue is limited to companies that fall under a specific surveillance law called "FISA 702". This law only applies to "electronic communication service providers" (like Facebook, Google or Microsoft), but does not apply to "traditional businesses" like airlines, hotels, trade, finances and alike.

There is another issue around a surveillance authorization called "EO 12.333", which allows the US to conduct surveillance in any business sector, including transatlantic cables outside of the United States. This is mainly relevant for the "Privacy Shield" assessment.

Overall, a suspension of data transfers under the SCCs is only necessary for companies that fall under FISA 702, which was introduced in 2007. The problem can be solved by fixing this law in the US.

- **Did Mr Schrems sue Facebook twice?**

While Mr Schrems has filed the original complaint with the DPC in 2013, the DPC has paused this procedure and filed a lawsuit *against* Facebook and Mr Schrems. They are *defendants* and have not started this (second) reference to the CJEU. In fact, Mr Schrems and Facebook have both opposed the reference to the CJEU for different reasons.

- **What does this case have to do with the "Privacy Shield"?**

Facebook has raised the "Privacy Shield" in the case, as they argue that the European Commission has approved US surveillance laws in the Privacy Shield and this assessment should also be binding when US surveillance laws are assessed under the SCCs. Mr Schrems has argued that this assessment is factually incorrect and the Privacy Shield is therefore invalid.

It is unclear if the Advocate General will address either argument, tough the Judges were intensively questioning the European Commission on the Privacy Shield during the oral hearing.

- **Why do you say that the SCCs are okay, but the Privacy Shield is not?**

The SCC is a generic tool for about 200 countries in the world. It does not deal with US surveillance laws. If there is a conflicting law, Article 4 of the SCCs allow the DPC to stop the data transfer. The SCCs therefore have an answer for the problem before the Court. In the Privacy Shield decision, the European Commission explicitly held that US surveillance law is compliant with EU law, which we fundamentally disagree with.

- **What do you think should have been done by the DPC?**

Under Article 4 of the SCCs, any data protection authority (like the DPC) can stop data transfers, if the SCCs are not factually complied with. Facebook Ireland was aware of NSA surveillance since at least 2013, but has not taken any measures to stop or limit the data transfers. In such cases, the regulator has to step in and take action.

- **How can companies comply with a favorable ruling?**

First, they would need to identify if any of their data goes to a US "*electronic communication service provider*" that falls under FISA 702. Most traditional industries do not fall under these surveillance laws, but large tech companies that many of us use (like Facebook, Google, Amazon or Microsoft) do.

Even if data goes to one of these providers, most essential data transfers (e.g. sending emails, direct messages or booking data) can still be transferred under so-called "derogations" in GDPR. In cases of mere "outsourcing" however, European companies may have to find alternatives outside of the US.