TOLERATING AMBIGUITY: REFLECTIONS ON THE *SCHREMS II* RULING

SUSANNA LINDROOS-HOVINHEIMO*

This paper considers the European Court of Justice's Schrems II ruling from a variety of angles. From a strictly legal point of view, considering the GDPR, the CJEU came to a logical conclusion. In this paper, I nevertheless try to think about other ways of understanding the dispute and the ruling. In addition to data protection law, the case is about surveillance, platform power, resistance, global politics, data territoriality and the Court's competence. These sensitive issues come forth when the strict data protection issues are set aside and a slightly more open analysis undertaken. In the end, however, the ruling does bring about real-life problems that pertain to data protection law. Transfers of data to third countries are a pressing problem that no one seems to know how to solve.

1 INTRODUCTION

On 16 July 2020, the Court of Justice at the European Union (CJEU) gave a preliminary ruling in the so-called *Schrems II* case.[1] The request had been made by the High Court in Ireland and concerned the legality of data transfers by Facebook Ireland to Facebook Inc., that is, transfers from the EU to the US.

The ruling is rather complex, and here my focus is only on certain key aspects. Firstly, the EU Court decided that the matter falls under EU law and the GDPR[2] because it does not concern Member States' national security. Secondly, the Court found that the Commission's decision on guidelines for Standard Contractual Clauses (SCCs)[3] is valid. These clauses are one means by which personal data can lawfully be transferred to third countries. The third conclusion by the Court – and the one that has received the most attention – concerns the Commission's Privacy Shield decision on the adequacy of data

* Professor, Faculty of Law, University of Helsinki (Finland). This article is based on a presentation delivered at the seminar *Schrems II and its Practical and Theoretical Consequences* held in Lund 16 September 2021, which was organised by Xavier Groussot. I thank Professor Groussot and Lund University for the kind invitation to participate.

[1] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Schrems II)* ECLI:EU:C:2020:559.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR) [2016] OJ L 119/1.

[3] Commission Decision 2010/87/EU on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council [2010] OJ L39/5, as amended by Commission Implementing Decision 2016/2297 (SCC Decision) [2016] OJ L344/100 in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights has disclosed nothing to affect the validity of that decision.

protection rights provided by the US.[4] The Court found that the decision is invalid because the US does not provide adequate protection.

From a data protection point of view, there is little to criticise in the judgment – if one belongs to the majority of academic data protection lawyers, who see the right to personal data as a good thing. In this ruling, the Court takes a logical step in the direction in which data protection law has been developing for a long time. The argumentation picks up where the first *Schrems* ruling[5] left off. There are no real surprises. The Court's reasoning respects the law – the GDPR – and provides no innovative or radical interpretations. The legislators' wishes were heard.

The legislators have been active indeed. Data protection is one area of fundamental rights protection areas – perhaps even *the* area – in which the Union has really made a difference. Our right to privacy would look very different if it were not for the active steps that the EU has taken. The individual's right to personal data is almost a trump card now; when it is in danger, the law does not hesitate. Many political and ideological obstacles have been overcome to achieve this level of protection and it stays strong under the Court's watchful eye. The *Schrems* rulings are one indicator of this general trend.

However, on closer inspection, the case proves puzzling. In this paper, I offer impressions of what the case is about, as well as what it brings about.

So, what happens in the case? There are several alternatives for interpreting it. The dispute touches on surveillance, data transfers, platform power, data protection authorities' duties, resistance, global politics, data territoriality, individualism, as well as the Court's competence. And it brings about a situation wrought with ideological, political and practical problems. In my view, the ruling of the EU Court seems to be riddled with ambiguities and it leaves quite a few questions unanswered.[6]

2 SURVEILLANCE OR SURVEILLANCE CAPITALISM?

I situate this analysis within the conceptual landscape of surveillance capitalism. In Shosanna Zuboff's critique,[7] massive data gathering causes privacy intrusions that produce new forms of capitalist exploitation. She calls this surveillance capitalism. A new kind of economic gain is derived from data, especially personal data. Tech giants, but also other kinds of commercial operator, are the ones to blame. They exploit us and turn our private information into data that has commercial value. Ever more efficient marketing of goods and services is their primary target, and they do not even shun brainwashing for consumerist purposes.

---

[4] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection [2016] OJ L 207/1 provided by the EU-US Privacy Shield is invalid.

[5] Case C-362/14 *Maximillian Schrems v. Data Protection Commissioner* (*Schrems I*) ECLI:EU:C:2015:650.

[6] For interesting analyses, see also, eg, Maria Helen Murphy, 'Assessing the implications of *Schrems II* for EU–US data flow' (2021) International and Comparative Law Quarterly 2021 1; Jockum Hildén, 'Mitigating the risk of US surveillance for public sector services in the cloud' (2021) 10(3) Internet Policy Review 2; Roisin Aine Costello, '*Schrems II*: Everything Is Illuminated?' (2020) 5 European Papers 1045; Andraya Flor, 'The Impact of *Schrems II*: Next Steps for U.S. Data Privacy Law' (2020-2021) 96 Notre Dame Law Review 2035; Jan Xavier Dhont, 'Editorial, *Schrems II*. The EU adequacy regime in existential crisis?' (2019) 26(5) Maastricht Journal of European and Comparative Law 597.

[7] Shoshana Zuboff, *The Age of Surveillance Capitalism – The Fight for a Human Future at the New Frontier of Power* (London: Profile Books 2019).

However, what Mr. Schrems is after in the *Schrems* cases at the CJEU is to combat something else. His ultimate critique is directed towards the surveillance authorities of third countries, most specifically the US. He is concerned with the widespread privacy breaches that are perpetrated by spying agencies. It is noteworthy that the *Schrems* rulings are not aimed at hindering surveillance capitalism, but surveillance as such, the kind of surveillance that government institutions do mainly for national security purposes. Neither Mr. Schrems nor the Court have a problem with the massive data gathering that Facebook does in Europe. Transferring data overseas is the problem.

Hence, in a surveillance capitalist framework we see that capitalism comes away unscathed. The traditional version of surveillance is the target here, not the surveillance capitalism for economic profit that Zuboff describes. Mr. Schrems has nothing against that. Hence, the set-up of the *Schrems* cases amounts to the conclusion that it is fine if Facebook does the surveillance in Europe, but it is not fine if public authorities in the US have unlimited and unchecked powers to access the data for their surveillance purposes.

The scenario can be compared with the German Facebook competition law case,[8] and the Commission investigation[9] into Facebook's actions on the European market. In these proceedings, it is assessed whether Facebook violates EU competition rules. According to the German authorities, Facebook collects user and device-related data from sources outside of Facebook and merges it with data collected on Facebook, which constitutes an abuse of a dominant position on the social network market in the form of exploitative business terms.[10] This legal perspective on Facebook's operations has emerged recently and is more closely tied to the critique of new forms of capitalism than the *Schrems* cases. In this sense, the *Schrems* rulings may be slightly disappointing. They provide no real objection to the capitalist operations of large platform companies.

3 LEGAL BASIS

It is interesting to note that a large part of the disagreement between Mr. Schrems and Facebook concerns the legal basis for the data transfers. Let us remind ourselves of how the story started. First, in 2013, Mr. Schrems made a formal complaint to the Data Protection Commissioner in Ireland that Facebook Ireland unlawfully outsources data processing operations to Facebook Inc. (Facebook Ireland's parent company). In 2013 the Data Protection Commissioner refused to investigate the complaint, arguing that it was bound by the Safe Harbour Decision made by the Commission. This decision allowed for data transfers to the US. Mr. Schrems initiated proceedings against the Data Protection Commissioner, and the High Court made the first reference to the CJEU.

In the *Schrems I* ruling from 2015, the EU Court invalidated the Safe Harbour Decision. Following the judgement, the High Court remitted the matter back to the Data Protection Commissioner who should investigate 'promptly with all due diligence and speed'.

---

[8] Case C-252/21 *Facebook Inc. and Others v Bundeskartellamt* (pending).

[9] See, eg, European Commission, 'Antitrust: Commission opens investigation into possible anticompetitive conduct of Facebook' (4 June 2021) <https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2848> accessed 30 September 2021.

[10] Compare with the recent ruling in Case T-612/17 *Google LLC, formerly Google Inc. and Alphabet, Inc. v European Commission (Google Shopping)* ECLI:EU:T:2021:763.

In November 2015, the Data Protection Commissioner informed Mr. Schrems that Facebook Ireland has in fact never relied exclusively on Safe Harbour as the legal basis for the data transfers. Months before the first case against the Data Protection Commissioner was filed in 2013, Facebook Ireland had in fact informed the Data Protection Commissioner that Facebook Ireland uses a number of means to legitimise the transfer, including consent and the use of SCCs. However, Mr. Schrems was not informed of this, nor apparently were the High Court or the EU Court. In fact, Mr. Schrems argues in the second case that the legal basis under which Facebook Ireland relies when transferring data remains unclear. Facebook Ireland had informed Mr. Schrems in 2015 that it now relies on SCCs, but also on several other legal means. Thus, Facebook Ireland seems to have changed its mind on which legal bases it relied on and was also hesitant to disclose them to Mr. Schrems.[11]

The discussion about legal bases is significant for various reasons. Firstly, the GDPR is quite explicit that there should always be a legal basis for processing. Of course, there can, be many. The controller, Facebook Ireland in this case, needs to be very clear in its decision on the basis on which in it relies. Secondly, the data subjects (that is, the people whose data is being processed) generally have a right to know the legal basis.

We see that the legal basis for transfers is a crucial issue in the dispute. However, the legal basis for Facebook's operations inside the EU is not. What is the legal basis? Contract or consent are possible options. However, they can both be contested because the GDPR puts specific weight on the control of the informed data subject. It may be unclear to most Facebook users what they are giving their consent to when agreeing to Facebook's terms.

Nevertheless, this dispute is not about the fact that Facebook gathers data, even though it could be about that. It is about the surveillance apparatus of the US. Mr. Schrems' complaint concerns only the fact that Facebook Ireland outsources personal data to the US, although there is no need to do so, when it is subject to electronic surveillance law such as FISA 702.

Note, though, that Mr. Schrems is not unhappy with all transfers to the US. He clarifies in his observations to the CJEU that his complaint does not raise the matter of the data protection level in the US as a whole. The electronic surveillance law (FISA 702) only applies to 'electronic communication service providers'. It does not apply to all other US industries, such as banks, trade, or airlines. Hence, Mr. Schrems argues that there are many situations in which EU data controllers can rely on instruments like the SCCDs to transfer data to the US, when no conflict between EU and US law arises. In addition, his complaint does not concern personal data that Facebook Ireland must send to the USA, such as messages that a European Facebook user sends to a friend over there. The complaint is limited to outsourcing of data processing operations that could just as well be processed within the EU.[12]

Facebook, on the other hand, argued that the US does indeed provide adequate access to judicial remedies:

> The US is a constitutional democracy with a centuries-old history of adherence to the rule of law, robust judicial review, and multi-layered protections to guard against

[11] See written observations of Maximilian Schrems in Case C-311/18 *Schrems II* (lodged on 31 August 2018), 1-2.
[12] ibid 2-3.

> governmental abuses of power. A decision that the US legal system does not ensure sufficient protection would not only affect data transfers to the US, but would likely imperil data transfers to the vast majority of other States, potentially including some benefitting from adequacy findings under Article 25 of the Directive.[13]

The US argued similarly.[14] Understandably, they did not admit that there would be problems with legal safeguards. They saw the US system as comparable to the ones used within the EU.[15] According to the US, the protection of personal data relating to national security data access adopt a holistic approach and afford protections for privacy. After personal data is transferred to a business in the US, any US government national security demand to disclose the data must be based on statutory authority, require adequate justification, and be targeted at a specific person. When data is acquired, it is subject to detailed data-handling procedures. There is a multi-layered system of checks, including independent oversight by the executive branch, the legislature, and the judiciary. The US also referred to the judicial remedies provided for individuals to access information about themselves, as well as possibilities for redress for unlawful intelligence activities by the government.[16]

We see in the observations by Facebook and the US that they argue in strong terms that the US system provides just as much protection for personal data as EU law does. They also point out that the legal system as a whole allows individuals access to various judicial remedies. However, the CJEU was not convinced.

4 RESISTANCE

The *Schrems* cases took a long time. They attest to the fact that legal proceedings are time-consuming, burdensome and of course expensive. The burden is especially large for private individuals and other small actors. The amount of work that Mr. Schrems and his lawyers had to put in is quite remarkable. Even after the first *Schrems* ruling from the CJEU, the Data Protection Commissioner refused to stop the transfers, which was Mr. Schrems' main objective. Instead, it started a quite baffling procedure. In 2016, it decided to file a lawsuit against Facebook Ireland and Mr. Schrems before the High Court, arguing that it has doubts about the validity of the Commissions SCC decisions.[17] With this, the investigation of any other matters raised by the complaint was again paused by the Data Protection Commissioner.

---

[13] Written observations of Facebook Ireland Ltd. in Case C-311/18 *Schrems II* (lodged on 3 September 2018), 4.

[14] The High Court admitted the US as *amicus curiae* in the main proceedings. The aim was to provide the High Court an accurate and up-to-date account of US privacy protections relating to national security access to EU individuals' data after transfer to the US. Also the CJEU gave the US this opportunity.

[15] On this, see also Marc Rotenberg, '*Schrems II*, from Snowden to China: Toward a new alignment on transatlantic data protection' (2020) 26(1-2) European Law Journal 141.

[16] See written observations of the United States of America in Case C-311/18 *Schrems II* (lodged on 31 August 2018), 5.

[17] Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC [2001] OJ L181/19; Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries [2004] OJ L385/74; Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council [2010] OJ L 39/5; (collectively - the 'SCCDs').

The Data Protection Commissioner maintained that any other matter or legal basis that Facebook Ireland may rely on can be dealt with at a later stage. Understandably, this was not what Mr. Schrems had hoped for. After five years without even a first decision by the Data Protection Commissioner, this approach opens the opportunity for never-ending attempts to shift the responsibility to the CJEU by requesting a preliminary ruling for each legal basis contained in Chapter 5 of the GDPR. In effect, Mr. Schrems argued that the DPC ignored its obligation to act on its findings following the investigations into Mr. Schrems' complaint.[18]

Mr. Schrems did not give up, and eventually his side of the story became the one that the CJEU mostly agreed with. Therefore, another theoretical lens through which to analyse the *Schrems* saga is resistance. In political philosophy, it is sometimes seen that law, and legal practices, facilitate little resistance. Instead, law is understood as the instrument to uphold the *status quo* of society and to legitimise possible power imbalances. Above all, this kind of thinking stems from the Marxist traditions of critical legal scholarship.[19]

This case may prove an exception, though. It presents an opportunity to see the emancipatory potential of law. The legal arena can be the scene for political battles. To me, this is one illustrative example of law becoming the space and the means for resistance.

What is so marvellous about this case is the role that Mr. Schrems is allowed to play. He becomes the champion of quite a large battle, in which he is not fighting for his own rights but trying nothing less than to make the world a better digital place. In its own way, the CJEU facilitates this battle.

Mr. Schrems is an activist. A statement by him a year after the *Schrems II* ruling shows that he continues the work because the decision has not had the desired effect:

> Over the last year, it seems that the relevant stakeholders have mainly engaged in deflection and finger pointing, each passing on responsibility to the next. Only a fraction of European businesses have realised that the underlying conflict between EU data protection and US surveillance law will not be solved in the short-term, and have moved towards hosting personal data in Europe, or other safe regions, instead of engaging in an endless compliance nightmare over US law. Other European companies regularly complain about a lack of 'guidance' despite two clear judgments. When guidance is given, such as the recent EDPB guidelines, many argue that it is 'unrealistic' to follow the requirements of the law […].[20]

5 IS DATA LOCALISATION THE INTENDED OUTCOME?

What we are left with after both *Schrems* decisions are insecurities. The SCCs are still one option for data transfers, even though not a viable option for many US companies because the CJEU has now ruled that the US legal system does not include the necessary protection. Nevertheless, the GDPR recognises that there may be situations in which non-EU countries provide an equivalent level of data protection. There are countries, where national law is

[18] See written observations of M Schrems in *Schrems II* (n 11) 3, 35-36.
[19] See on this discussion for example the ways in which Jacques Rancière's thinking has been applied in law. Monica Lopez Lerma, Julen Etxabe (eds), *Rancière and Law* (Oxon: Routledge 2019).
[20] Statement by Max Schrems on the "*Schrems II"* Anniversary' (*NOYB*, 16 July 2019) <https://noyb.eu/en/statement-max-schrems-schrems-ii-anniversary> accessed 18.10.2021.

similar to EU law (for instance Switzerland, Israel, and Canada) and companies can voluntarily commit to EU principles by signing SCCs. US companies, on the other hand, should rely on one of the contractual options in Articles 46 to 48 of the GDPR for outsourcing. However, for companies that fall under US surveillance laws, most options are practically impossible, as US law was not deemed adequate by the CJEU.

In sum, there are not many viable legal options for certain companies to transfer data to the US. This pushes the interpretation of the judgement towards a view where data should be held in Europe and not transferred at all. However, it can be asked whether data localisation can be a solution in today's digitalised world. As Chander puts it,

> First, keeping the information in the EU does not insulate the data from the surveillance of the European Member States' own intelligence services. Second, keeping data in the EU does not insulate it from data sharing by European intelligence services with the USA. Third, if the goal of the GDPR is to assure that the foreign protection is 'essentially equivalent' to that available under EU law, it seems fair to ask whether the Member State surveillance law is markedly more protective, if the shoe were on the other foot.[21]

Fourth, the US intelligence services seem quite able to do their surveillance in Europe even if the data remained here.

So, what is the fight really about? It is probably about power. But it may just be that the surveillance organisations have so much of it anyway that no court case can really change that. To stop data transfers to the US may just be one small detail in a very large picture, one in which data is being processed by surveillance agencies in all countries anyway.

If data localisation is the outcome of the *Schrems* cases, then it does not seem like a practical solution, nor is it perhaps the solution anyone was looking for to combat privacy intrusions by surveillance authorities. It certainly makes life difficult for many companies.

6 DATA TERRITORIALITY – AN OUTDATED NOTION?

In the GDPR context, the logic is that data always reside somewhere. This may be an outdated notion, yet it informs these cases, too. It seems odd in today's digital landscape that data would exist in a place, or that it needs to be physically moved.

Rather, one wonders whether the internet could be understood as a limitless space, where data moves freely in all directions all the time. After all, Facebook Ireland does permit my friends in the US to access my data. My American friends can usually see everything I post, and that way the data are also accessible to the surveillance agencies. Likewise, a hotel in New York will need to collect my data if I make a booking. A book shop in the UK will do the same. If a family member of mine has lived in a third country and then dies, the authorities of both countries will have to exchange various data. The relatives will need some from the third country as well, in order to manage the deceased's estate. Is it a realistic legal solution that all such access across borders constitutes a data transfer subject to the GDPR

[21] Anupam Chander, 'Is Data Localization a Solution for Schrems II?' (2020) 23(3) Journal of International Economic Law 771, 781.

Chapter 5?[22] How all the different legal bases are really supposed to work and which of them is suitable for the various global communications taking place in different situations is all but clear. It may be that the whole notion of data transfers and the set-up for their legal bases is too impractical for real-life use. One reason surely is the territoriality notion. To think that my data on Facebook would exist only inside the EU is simply misleading. It exists everywhere I share it.

Where is the space in which the internet is? And what kind of space is it? In trying to tackle these issues, current legal thinking easily stumbles on its own boundaries. Law, even transnational law, simply does not have the tools to grapple with the non-territoriality of the internet. One is reminded of Foucault's idea of *heterotopia*:

> There are also, probably in every culture, in every civilization, real places – places that do exist and that are formed in the very founding of society – which are something like counter-sites, a kind of effectively enacted utopia in which the real sites, all the other real sites that can be found within the culture, are simultaneously represented, contested, and inverted. Places of this kind are outside of all places, even though it may be possible to indicate their location in reality. Because these places are absolutely different from all the sites that they reflect and speak about, I shall call them, by way of contrast to utopias, heterotopias.[23]

The internet is a site of its own, a place like no other, yet a real place in the sense that it does exist. It is not an imaginary space or a metaphor, rather, it is an existing site where many things happen with real, tangible effects. But it does not exist anywhere and is therefore outside all places. It is absolutely different from the places which it reflects.

Moving data around the internet could be seen as moving it within one place, a place of its own, even though the data simultaneously may move across the borders of traditionally-conceived legal places, states. However, there is a clear discrepancy between the spatiality of the internet and the territoriality of states' jurisdiction, and it brings this case a certain uncanny flavour. The fight is about data being moved but only about certain data being moved in certain specific situations in which it might end up in the wrong hands. At the same time, data moves all the time by other means and other actors into all kinds of hands on both sides of the Atlantic and beyond.

7 PERSONAL DATA IS PURELY INDIVIDUAL – DEFINITELY AN OUTDATED NOTION

Every conversation on Facebook, every comment and every press on the 'like' button includes personal data of at least two people: mine and my friend's, with whom I interact. Communication takes two.

[22] One option for Facebook Ireland and Facebook Inc. would perhaps be to argue that they are one and the same controller (or, perhaps, joint controllers), whose operations revolve around the same data sets (and happen in Europe). There would be no need for data localisation, nor any transfers; the data would just be in the hands of them both from the beginning. This scenario was not discussed in the *Schrems II* judgment.
[23] Michel Foucault, 'Of Other Spaces' (1986) 16(1) Diacritics 1986 22, 24.

The individualist ideology that data protection law builds upon is problematic for many reasons, but this is one of them.[24] It is extremely hard to delineate where my data begins and another person's ends when we are dealing with communication and interaction. Communication is simply not compatible with the notion of separate individuals' personal data staying separate, even though the GDPR often seems to require this.

According to the GDPR, personal data is any data that relates to identified or identifiable individuals. This is the key feature of the Regulation and it defines the scope of data protection law in the Union. Only data that can be linked to an individual is protected.[25] On the other hand, any kind of data that can be linked to an individual is protected. The data does not have to be sensitive nor personal in any way. Also, publicly available data fall within the scope of the Regulation.

The individualist starting point of data protection law is prominent, whereas protection of private life is a much broader – and older – legal concept. The protection of privacy, private life and correspondence, which are found in most European constitutions, can conceptually include protection of groups – such as families – from unwanted intrusion. The more traditional forms of privacy protection were about the home and the private sphere of the household. These do not aim solely at protecting an individual. Much has changed. Today, when the legal focus on privacy protection lies on personal data, the emphasis of privacy rights is very much centred on individuals.

There are continuous problems when data protection rules are applied to something for which they do not really fit. A non-technological example is the *Nowak* case also from the CJEU, which includes difficulties in applying data protection rules to data that constituted the personal data of two people.[26] In this sense, the *Schrems II* judgement takes no steps towards clarification, but leaves us with ambiguities that no-one knows how to solve.

How does the Court, then, decide on the case? By focusing on Mr. Schrems, the individual. It is the protection of him that drives the Court's reasoning. The protection of his rights opens up the case procedurally and also as regards competence. His rights are the aim that override all else. Transfers cannot be allowed. Here the Court seems to argue that it has no leeway because otherwise there would be a loophole in the protection of rights.[27] The teleology of the GDPR dictates the outcome of the case: the individual must be protected.

It may be that the Court's conclusions are the best ones possible, and it may be that they are the only ones to satisfy the wishes of the legislators who drafted the GDPR. Nevertheless, they do leave us with the question of whether data protection legislation is ideal in its current, individualised form. To protect the fundamental right to personal data is naturally the right thing to do, but to construct both the data and the people in strictly individualised ways may prove problematic in future case law.

---

[24] For critique of individualism in privacy protection, see Susanna Lindroos-Hovinheimo, *Private Selves: Legal Personhood in European Privacy Protection* (CUP 2021).

[25] See, eg, Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* ECLI:EU:C:2016:779.

[26] Case C-434/16 *Peter Nowak v Data Protection Commissioner* ECLI:EU:C:2017:994.

[27] See *Schrems II* (n 1), especially para 105. For similar teleological reasoning, see Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* ECLI:EU:C:2018:388.

8 COMPETENCE AND JURISDICTION

The Court clearly has jurisdiction, as the whole data protection regime rests solidly on the TFEU and the Charter. Hence, there should be no problem with formal legitimacy of the Court's ruling.

Nevertheless, the Court has to deal with questions about competence because some of the parties, especially Facebook, argue that the Court does not have the required amount of it:

> The application of EU law to the transfer of data from the EU to third countries is not disputed by Facebook. However, the implicit assumption underlying the High Court's findings is that the Directive's provisions apply in respect of processing operations relating to State security activities within the EU, notwithstanding (i) the lack of Union competence by virtue of Article 4(2) TEU and (ii) Article 3(2) of the Directive excluding operations concerning State security from the Directive's scope.[28]

The argument is that because national security matters fall outside the reach of EU competence in accordance with Article 4(2) TEU, the EU Court cannot in fact engage in a proper comparison of US regulation and European security regulation. This way, the claim is that the Court does not have the jurisdiction to assess the national security regulation of third countries.

This is an interesting argument, but it does not succeed. The Court reasons in a teleological manner pointing out that it has full competence because without it, data protection in the EU could not be considered in full. Therefore, even though the Court may not have jurisdiction to assess the legality of European national service regimes, it does have jurisdiction to assess the remedies afforded by US law in this area.

For the outcome of the case, it becomes decisive that the Court is not convinced that the US legal system provides enough protection for individuals. In this assessment, the Court also indirectly considers the protection afforded in European security regimes. However, this does not diminish the competence of the Court, according to the Court, because that rests on EU data protection law.

The CJEU considers several statements about the US legal system and its various options for remedies. From a procedural point of view, it is quite interesting that even though this is a preliminary reference ruling, much of the reasoning does indeed concern facts. The CJEU has a lot to say about the actual practicalities of data transfers. It is understandable within the context of the case, but does go against the traditional view of EU law, according to which the CJEU does not rule on facts in preliminary rulings. In addition, many parts of the judgment concern evaluation of another legal system, and they get similar significance as the facts of the dispute. This is one illustration of how other matters than strictly data protection law come to be intertwined in the case.

[28] Written observations of Facebook Ireland Ltd in *Schrems II* (n 13) 3.

9 CONCLUSIONS: AMBIGUITIES

There are two aspects that I would like to highlight by way of concluding this discussion. The ruling caused a lot of debate and has been criticised in many fora. The attention it got is striking, considering that: (a) the ruling only concerns certain data transfers in certain contexts, and (b) the ruling is faithful to data protection rules as they are defined in the law. Hence, it may be that much ado has been caused by some other factors, most likely political ones. It is certainly understandable that a European Court deciding that US law is not good enough could be considered to be rude.

When analysing this decision – any decision – in a critical manner, it is nevertheless prudent to consider alternatives. Could the Court have decided the case in another way? What way could that have been?

I argue that the Court came to the only logical conclusion. The data protection rules are what they are and when applying them in this context, the Court reached a legally sound decision. The legislators' wishes were respected and the fundamental purposes of data protection law, as they are defined in case law today, were upheld. The Court really did not have any choice.

In the end, this is quite a technical data protection case. The commotion it has caused has most likely been about things other than just data protection law. In this paper, I have offered suggestions on what those things could be. The case is about surveillance, platform power, resistance, global politics, data territoriality and the Court's competence, among other things. These are sensitive issues.

The results of the choices that the Court makes cannot be ignored. The consequences are significant. There is still no clarity on data transfers to the US and the diplomatic endeavours to create a mutual framework have not progressed. The Court's ruling has left us with a real-life dilemma that is hard to solve because of political pressure and national self-interests – not an unusual situation in EU law, I suppose. The Court may not be a legislator as such, but its decisions prompt legislative solutions that are needed urgently. At present, we are left with ambiguities.

LIST OF REFERENCES

Chander A, 'Is Data Localization a Solution for Schrems II?' (2020) 23(3) Journal of International Economic Law 771
DOI: https://doi.org/10.1093/jiel/jgaa024

Costello R A, '*Schrems II*: Everything Is Illuminated?' (2020) 5 European Papers 1045

Dhont J X, 'Editorial, *Schrems II*. The EU adequacy regime in existential crisis?' (2019) 26(5) Maastricht Journal of European and Comparative Law 597
DOI: https://doi.org/10.1177/1023263x19873618

Flor A, 'The Impact of *Schrems II*: Next Steps for U.S. Data Privacy Law' (2020-2021) 96 Notre Dame Law Review 2035

Foucault M, 'Of Other Spaces' (1986) 16 Diacritics 22
DOI: https://doi.org/10.2307/464648

Hildén J,'Mitigating the risk of US surveillance for public sector services in the cloud' (2021) 10(3) Internet Policy Review 2
DOI: https://doi.org/10.14763/2021.3.1578

Lindroos-Hovinheimo S, *Private Selves: Legal Personhood in European Privacy Protection* (CUP 2021)
DOI: https://doi.org/10.1017/9781108781381

Lopez Lerma M and Etxabe J (eds), *Rancière and Law* (Oxon: Routledge 2019)
DOI: https://doi.org/10.4324/9781315666563

Murphy M H, 'Assessing the implications of *Schrems II* for EU–US data flow' (2021) International and Comparative Law Quarterly 1
DOI: https://doi.org/10.1017/s0020589321000348

Rotenberg M, '*Schrems II*, from Snowden to China: Toward a new alignment on transatlantic data protection' (2020) 26(1-2) European Law Journal 141
DOI: https://doi.org/10.1111/eulj.12370

Zuboff, Shoshana, *The Age of Surveillance Capitalism – The Fight for a Human Future at the New Frontier of Power* (London: Profile Books 2019).