Dan Jerker B. Svantesson
Bond University, Australia
dasvante@bond.edu.au
ORCID: 0000-0003-2106-5594

https://doi.org/10.26881/gsp.2021.4.02

International Data Transfers post *Schrems* – Moving Towards Solutions

The statement that the modern world depends on international data transfers is difficult to dispute. However, the statement that international data transfers may undermine the protection of personal data is equally difficult to dispute. In this we see both a problem and a desired outcome. The problem we see is a clash between two important objectives. Or more precisely, we see a clash between, on the one hand, an important multifaceted objective and, on the other hand, the protection of a complex fundamental human right with implications going far beyond that right itself. The desired outcome we see is that we, somehow, must facilitate data privacy respecting international data transfers.

The above ought to be relatively uncontroversial. However, as soon as we move towards the obvious question that flows from the above – namely that of *how* we can facilitate data privacy respecting international data transfers – we enter a territory best described as a combination of a minefield and a quagmire. To make progress in such an environment we must proceed with caution and yet avoid getting bogged down in the unavoidable challenges, such as definitional challenges, we will face.

In this article, I will seek to canvass a selection of key considerations that ought to be kept in mind when we discuss approaches to international data transfers. However, to prepare ground for that discussion, I will first set the scene by examining the so-called *Schrems II* decision, its larger context and background, as well as some of the reactions we have seen to that decision.

Finally, by way of introduction, I wish to make clear that I have opted not to provide any overview of the applicable legal provisions as such.[1] Just restating – without any commentary – the relevant provisions (art. 44–50) of the General Data Protection Regulation[2] (GDPR) would have taken up just under 3,000 words, or approximately

[1] See instead: Ch. Kuner, *Articles 44–50 Chapter V* [in:] *The EU General Data Protection Regulation (GDPR): A Commentary*, eds *idem et al.*, Oxford University Press 2020, pp. 755–862.

[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), OJ 2016 L 119/1.

50% of the space of this article. This illustrates the considerable complexity with which this area of law is associated.

1. Generally about international data transfers

Protecting privacy, including data privacy, is not optional. Rather it is necessary to always keep in mind that we are dealing with a fundamental human right. This, in itself, imposes limitations on what solutions can ever be regarded as acceptable. And as hinted at above, in the right to data privacy, we find a right that is complex – indeed, hard to define and delineate – and that is an important enabler of other human rights. Indeed, the protection of data privacy is an essential feature of any democratic form of governance.

The protection afforded by national data privacy laws is easily circumvented if the personal data they are meant to protect can be transferred to third countries without appropriate controls, safeguards and limitations. This is the most obvious and undisputable justification for the restrictions that data privacy laws commonly impose on international data transfers. At the same time, as observed already in the introduction, the societies we have built are now interacting to such a degree that crucial aspects would grind to a halt if personal data were not allowed to be transferred between countries. Writing an article in 2016 commenting on the *Schrems I* decision, I described this tension as the first of the many Gordian knots that characterise this area of law.[3]

The Covid-19 pandemic, that still holds the world in its grip at the time of writing, has showcased just how dependent we are on the Internet and its inherent cross-border data flows. However, this is of course by no means an issue specific to our online environment. International data transfers are also common – not to say essential – in many other settings such as international travel, international trade, employment records in multinationals, and in relation e.g., to research and health data.[4]

The need to strike a balance that upholds the right to privacy in an enforceable rather than symbolic manner, and that generates justified rather than blind trust is obvious.

[3] D. Svantesson, "Cross-border data transfers after the CJEU's Safe Harbour Decision – A tale of Gordian Knots," *Alternative Law Journal* 2016, no. 41(1), pp. 39–42.

[4] For a discussion of transborder health data flows, including research data, see e.g.: D. Mascalzoni, H.B. Bentzen *et al.*, "Are Requirements to Deposit Data in Research Repositories Compatible With the European Union's General Data Protection Regulation?," *Annals of Internal Medicine* 2019, no. 170(5), pp.332–334; and H.B. Bentzen, D. Svantesson, "Jurisdictional Challenges Related to DNA Data Processing in Transnational Clouds," [in:] *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy*, eds D. Svantesson, D. Kloza, Intersentia Ltd 2017, pp. 241–260.

2. Briefly about the lead up to *Schrems II*

The European Data Protection Supervisor (EDPS) has done us all a great favour by putting together and publishing its valuable "Case Law Digest" specifically on the topic of transfers of personal data to third countries.[5] This 10 June 2021 publication provides a structured and systematic overview of the case law developments that led us to where we are today.

I will not repeat that discussion here. Instead, I will limit myself to a very brief overview of the most important features of the three key cases that preceded *Schrems II* focusing on, and admittedly eclectic selection of issues I see as key to understanding this area.

2.1. Case C-101/01 *Lindqvist*

At the time of writing, the *Lindqvist* case is already turning 18 years old. However, conclusions reached in the case are still of significance. And since this matter dealt with issues somewhat different to those of the other authorities I will mention here, I will spend some time on this case. In *Lindqvist*, the Court concluded:

> There is no "transfer [of data] to a third country" […] where an individual in a Member State loads personal data onto an internet page which is stored on an internet site on which the page can be consulted and which is hosted by a natural or legal person who is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country.[6]

While this conclusion is interesting in its own right, it is also worthwhile to examine how the Court reached that conclusion. Having noted that "it is necessary to take account both of the technical nature of the operations thus carried out and of the purpose and structure of Chapter IV [GDPR Chapter V] of that directive where Article 25 appears,"[7] the Court made some observations as to the relevant technical setup. In particular it noted that, "Lindqvist's internet pages did not contain the technical means to send that information automatically to people who did not intentionally seek access to those pages."[8]

It is, of course, correct to note, as the Court did, that Lindqvist could not transfer the content of her website to an Internet user who was not connected to the Internet at the time, or who did not wish to take the steps necessary to visit her website. That is, however, equally true e.g., for TV broadcasts and the Court's justification of their approach, by reference to the relevant technology, is rather unconvincing. Further, we

---

5 European Data Protection Supervisor, *Case Law Digest: Transfers of personal data to third countries* (2021) https://edps.europa.eu/data-protection/our-work/publications/court-cases/case-law-digest-2021-transfers-personal-data_en [accessed: 2021.09.09].

6 Case C-101/01, *Bodil Lindqvist*, ECLI:EU:C:2003:596, p. 100.

7 *Ibidem*, par. 57.

8 *Ibidem*, par. 60.

may wonder how this relates to modern social media that indeed pushes content from one user to others who have the relevant app installed.

The Court then turned to the purpose of the relevant part of the Directive. In doing so, the Court observed that "Chapter IV of Directive 95/46 [GDPR Chapter V] contains no provision concerning use of the internet."[9] And went on to note that therefore "one cannot presume that the Community legislature intended the expression 'transfer [of data] to a third country' to cover" the type of Internet conduct in question.[10]

This conclusion is somewhat surprising. The fact that the Directive does not make specific mention of the Internet, suggests that it was drafted in technology-neutral language. Where that is the case, it cannot be assumed that the drafters did not intend the Directive to apply to Internet-related activities such as in the *Lindqvist* case. Rather, it seems at least equally likely that the technology-neutral language suggests that the application of the Directive should not be dependent on the technology in question.

Finally, and perhaps of broadest relevance, it is interesting to observe how the Court in the *Lindqvist* case, departed from a literal interpretation of the applicable law, and adopted a "consequence focused approach"[11] basing its decision in important respects on what would be the consequences of its decision:

> [i]f Article 25 of Directive 95/46 were interpreted to mean that there is 'transfer [of data] to a third country' every time that personal data are loaded onto an internet page, that transfer would necessarily be a transfer to all the third countries where there are the technical means needed to access the internet.

As the Court noted, this would necessarily turn the special regime provided for by Chapter IV of the directive into a regime of general application, as regards operations on the Internet.[12] This consequence focused approach is of great use in the technology law field, it is far too rare, and it ought to be more broadly adopted by courts (and indeed more consistently adopted by the Court of Justice of the European Union – CJEU).

2.2. Case C-362/14 *Schrems I*

Through a decision of July 2000, the European Commission made a finding that the US Safe Harbour scheme met the required adequacy level. This decision opened the door for extensive transatlantic data transfers.

The Safe Harbour regime can be seen as a pragmatic structure that managed to combine European data privacy traditions with the US tradition of data privacy as a consumer right. However, it was a structure that was built on sand; in fact, as the CJEU's decision in *Schrems I* shows, it was a structure for which a building permit

---

9 *Ibidem*, par. 67.
10 *Ibidem*, par. 68.
11 See further: D. Svantesson, "What is 'Law', if 'the Law' is Not Something That 'Is'? A Modest Contribution to a Major Question", *Ratio Juris* 2013, no. 26(3), p. 456.
12 Case C-101/01…, par. 69.

should never have been granted. Thus, as the main outcome of *Schrems I*, the CJEU held the Commission's July 2000 adequacy finding to be invalid, and it was made clear that transfers could no longer be made in reliance on the Safe Harbour scheme. Importantly, the Court emphasised that:

> Article 25(6) of Directive 95/46 implements the express obligation laid down in Article 8(1) of the Charter to protect personal data and, as the Advocate General has observed in point 139 of his Opinion, is intended to ensure that the high level of that protection continues where personal data is transferred to a third country.[13]

This highlights that the application of the provisions that regulate international data transfers is firmly guided by the EU Charter of Fundamental Rights (the Charter).[14] Furthermore, the CJEU ruled that a Commission adequacy finding:

> does not prevent a supervisory authority of a Member State [...] from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.[15]

Relatedly, the CJEU's judgment made clear that only the CJEU has jurisdiction to declare that a Commission adequacy finding is invalid. In addition, the judgment provided guidance as to the more precise meaning of a country providing an adequate level of protection:

> [T]he term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union.[16]

To conclude this section, it may be noted that, in *Schrems I*, the Court adopted a more formalistic approach to the law than it did in *Lindqvist*.

2.3. Opinion 1/15 *EU-Canada PNR Agreement*

The CJEU issued Opinion 1/15 in response to the European Parliament's request relating to an agreement envisaged between Canada and the European Union on the transfer and processing of Passenger Name Record data. The Court concluded that the draft agreement could not be concluded in its proposed form. Most importantly for our context, this conclusion was reached based on the observation that several of the agreement's provisions were incompatible with fundamental rights provided under the Charter. The Court referred to *Schrems I* and re-emphasised that the "right to

---

13 Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, ECLI:EU:C:2015:650, par. 72.
14 Charter of Fundamental Rights of the European Union, OJ 2000, C 364/01 and OJ 2010, C 83/389.
15 Case C-362/14…, par. 107.
16 *Ibidem*, par. 73.

the protection of personal data requires, inter alia, that the high level of protection of fundamental rights and freedoms conferred by EU law continues where personal data is transferred from the European Union to a non-member country."[17] Further, as noted by Kuner in his expert analysis of the matter, Opinion 1/15 indicates that the Court will hold international agreements to a strict standard of fundamental rights protection.[18]

3. Case C-311/18 *Schrems II* – overview, implications, and comments

When it became clear that the aftermath of the *Schrems I* case included a new mechanism – Privacy Shield – sharing many features with the abandoned Safe Harbour structure, the fact that there would be a *Schrems II* decision[19] was not surprising. Like the initial *Schrems I* matter, *Schrems II* was referred to the CJEU by the Irish High Court, and on this occasion the Irish court referred no less than 10 different questions to the CJEU.

In essence, the matter related to whether the US surveillance programmes interfered with the fundamental rights to privacy, to data protection and to effective judicial protection in such a manner as to render transfer of personal data to the US unjustifiable. To that end, the judgment addressed several issues. Importantly, the CJEU made clear that the GDPR:

> […] applies to the transfer of personal data for commercial purposes by an economic operator established in a Member State to another economic operator established in a third country, irrespective of whether, at the time of that transfer or thereafter, that data is liable to be processed by the authorities of the third country in question for the purposes of public security, defence and State security.[20]

Further, the Court held the Privacy Shield invalid, and concluded that: "data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded a level of protection essentially equivalent to that guaranteed within the European Union".[21]

The *Schrems II* decision resulted in intense academic debates.[22] From an international perspective, it is particularly interesting to note how the decision has been

---

17 *Ibidem*, par. 134.

18 Ch. Kuner, "International Agreements, Data Protection, and EU Fundamental Rights on the International State: Opinion 1/15, EU-Canada PNR," *Common Market Law Review* 2008, p. 55.

19 Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems*, ECLI:EU:C:2020:559.

20 *Ibidem*, par. 203.

21 *Ibidem*.

22 See e.g. Ch. Kuner, "Schrems II Re-Examined", *Verfassungsblog.de* 25 August 2020, https://verfassungsblog.de/schrems-ii-re-examined/ [accessed: 2021.09.09] and D. Korff, "Korff on Kuner: *Schrems II* Re-Examined," 3 September 2020, https://www.ianbrown.tech/2020/09/03/korff-on-kuner-schrems-ii-re-examined/ [accessed: 2021.09.09]; that purports to be a response to Kuner but that, in too large parts, rather appears intent on reading more into Kuner's statements than reasonable may be justified.

approached in the context of whether the conditions data privacy laws traditionally impose on transborder data transfers are properly viewed as measures imposing data localisation requirements. As to *Schrems II* Chander notes:

> I do not mean to suggest that *Schrems II* requires data localization or that it is even the recommended response. […] However, by failing to offer any guidance as to what such additional measures might be, it creates uncertainty. […] Thus, even while *Schrems II* does not establish a *de jure* requirement for data localization, its encumbrances on cross-border data flows to the United States, and to other foreign countries, seem to point many businesses to use data localization to solve the problems the decision poses.[23]

This is, of course, both an important and a correct observation. And perhaps it can be seen as a step back from Chander's earlier claim (with Le) as to data privacy laws: "While these laws are not explicitly designed to localize data, by creating significant barriers to the export of data, they operate as data localization measures."[24]

In my view, we gain nothing but confusion if we broaden the definition of data localisation so as to encompass by default the conditions data privacy laws traditionally impose on transborder data transfers. After all, there is a significant difference between something being banned and something only being allowed under stated conditions. More specifically in our context, there is a significant difference between a requirement mandating that data be stored or processed in a specific jurisdiction, on the one hand, and conditions being imposed on the transfer of data to another country, on the other hand. Thus, I have advanced the following, more narrow definition of data localisation: "'Data localisation' refers to a mandatory legal or administrative requirement directly or indirectly stipulating that data be stored or processed, exclusively or non-exclusively, within a specified jurisdiction."[25] With that definition in mind, I have recommended that "the conditions data privacy laws traditionally impose on transborder data transfers do not necessarily amount to data localisation."[26] I will have reason to return to the topic of data localisation in the below.

The CJEU's *Schrems II* decision has also led to intensive activity from the relevant European Union bodies.[27] At the time of writing, the most recent, development flowing from the *Schrems II* decision is the Commission's Decision of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. All these de-

---

[23] A. Chander, "Is Data Localization a Solution for Schrems II?", Georgetown Law Faculty Publications and Other Works 2020, 2300, p. 2, https://scholarship.law.georgetown.edu/facpub/2300 [accessed: 2021.09.09].

[24] A. Chander, U. Le, "Data Nationalism", *Emory Law Journal* 2015, vol. 64/3, p. 677, p. 718.

[25] D. Svantesson, "Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines", *OECD Digital Economy Papers* 2021, no. 301, OECD Publishing, Paris, p. 8, http://dx.doi.org/10.1787/7fbaed62-en [accessed: 2021.09.09].

[26] *Ibidem*, p. 26.

[27] See e.g.: EDPB – EDPS Joint Opinion 2/2021 on the European Commission's Implementing Decision on standard contractual clauses for the transfer of personal data to third countries for the matters referred to in Article 46(2)(c) of Regulation (EU) 2016/679.

velopments are deserving of detailed scrutiny. However, that goes beyond the scope of this article.

4. Selected key considerations as we move forward

So, are we stuck? The above might point to an impossible situation where there is no prospect of appropriate solutions that can both cater for international data transfers and at the same time, uphold a data privacy protection meeting the standards of the Charter. However, there are reasons to think that progress can, indeed, be made. Not least the old proverb that necessity is the mother of invention should give us hope. We quite simply must find solutions, and it would be useful for those solutions to be more long-term than was the temporary "patch" provided by the Privacy Shield.

In a publication stemming from my time in 2010 as a Visitor at the European University Institute, I explored options for reform in this field in some detail.[28] I will not repeat that discussion here. Rather, I will seek to bring attention to a range of considerations that ought to be kept in mind when we discuss approaches to international data transfers.

4.1. Identifying the "baseline" and the "zone of flexibility"

Discussions of balancing data privacy protection with other interest and rights are unpopular activities. And it is, of course, true that not all interests are equal and not everything is up for negotiation. Regardless of what trade advantages may be gained, data privacy cannot be traded away in a manner that undermines the data subjects' fundamental rights. In the immortal words of Spiros Simitis: "[t]his is not bananas we are talking about."[29] There is a "baseline" that must not be crossed.

At the same time, above this non-negotiable "baseline" set by human rights law, there is a "zone of flexibility". Within that zone we may pursue solutions that cater for all interests involved, and we may, indeed, pursue options that provide protection beyond the mentioned baseline, for example, by pursuing paths facilitating the adoption of privacy as a competitive advantage.

In my view, we need a more open discussion about what falls within the "baseline" and what fits within the "zone of flexibility".

4.2. The right level of granularity

As is clear already from this article, it is common practice to observe a tension between, on the one hand, the need for international data transfers, and, on the other

[28] D. Svantesson, "A legal method for solving issues of Internet regulation; applied to the regulation of cross-border privacy issues," *European University Institute Working Paper LAW* 2010, no.18.

[29] Cited by Lee Bygrave "International agreements to protect personal data" [in:] *Global Privacy Protection: The First Generationeds*, eds J. Rule, G. Greenleaf, Edward Elgar 2008, p. 15.

hand, the need for effective data privacy protection. However, in our context, that is perhaps an unhelpful "macro perspective". Perhaps we need to approach the considerations involved with greater granularity; that is, perhaps we are better served if we start analysing what types of international data transfers we are talking about, and what aspects of data privacy protection we are calling for.

Put simply, we can acknowledge the general value of international data transfers without assuming that all types of such transfers are of equal importance and value. Some such transfers – consider e.g., Opinion 1/15 – are important for the purpose of national security. Others are motivated by economic considerations such as "economies of scale". Yet others stem from technical structures that force us to consider whether it is current technological realities, or indeed the law, that is the proverbial "tail wagging the dog". It is not my aim here to assess how these grounds for international data transfers stack up when compared to data privacy interests. However, to me it seems crucial to acknowledge that not all current situations involving international data transfers are of equal importance.

Similarly, as alluded to, we must acknowledge the necessity of ensuring effective data privacy protection without assuming that all aspect of all data privacy laws are equally necessary for an adequate level of protection.

Admittedly, much work remains, and many severe challenges must be tackled along the way to solutions. For example, it may be noted that data typically is collected and transferred in bundles that contain both personal, and non-personal, data. This creates complications. However, already by moving into this greater granularity we ca move closer to a position in which the various objectives involved may be properly evaluated and either reconciled or at least balanced.

4.3. It takes two to tango

Where country A's data privacy law imposes conditions on international data transfers with the result that data cannot be transferred from country A to country B, it is commonplace to see country A's data privacy law as restrictive or even protectionist – it is country A's data privacy law that is blamed for the impossibility of the transfer. However, that is an unhelpful oversimplification. What we are faced with in any such a situation is a compatibility issue. Country A's and country B's laws are quite simply not compatible enough to facilitate the data transfer in question. Country B's inadequate data privacy protection is equally much the cause of the resulting barrier to data transfers. As the saying goes, 'it takes two to tango' and we will get no closer to solutions if we do not recognise this.

To my mind, this also has implications for discussions as to whether the restrictions data privacy laws commonly impose on international data transfers amount to 'data localisation'. If we recognise that the cause of the transfer being prevented is a compatibility issue, that lends support to the conclusion that the conditions data privacy laws traditionally impose on transborder data transfers do not necessarily amount to data localisation.

At any rate, if it is conceded that we are here dealing with a compatibility issue, we can usefully link into – and draw from – the discussion of "legal interoperability"[30] or the related concept of "jurisdictional interoperability".[31] Put simply, legal interoperability involves "the process of making legal norms work together across jurisdictions",[32] while the aim of jurisdictional interoperability is more modest and involves reaching a situation "where we have: (1) only a minimal level of serious jurisdictional clashes, and (2) an acceptable level of less serious jurisdictional clashes".[33] In a similar manner to how we now routinely work with privacy-by-design and security-by-design, perhaps the time has come to pursue "jurisdictional interoperability-by-design"?[34]

4.4. A "layered approach" facilitating interoperability

During the discussions that preceded that final version of the GDPR, I proposed what I termed a "layered approach" for the (territorial) scope determined in art. 3.[35] In essence my point was that, in the case of a diverse instrument such as the GDPR that contains both (virtually) globally accepted abuse-prevention provisions (the "abuse-prevention layer" e.g., Article 5), widely accepted rights (the "rights layer", e.g., Article 15), as well as bureaucratic administrative rules with few equivalents elsewhere (the "administrative layer" e.g., art. 37), it is inappropriate to apply the same threshold test for the applicability of all these rules to foreign parties. In other words, we need different tests regulating when such a party must comply with these rules, and we could cater for a lower threshold, and thus a wider reach for, the provisions of the "abuse-prevention layer" than for the other two layers. This thinking – if adopted in relation to application of the international data transfer rules – may have the potential to contribute towards the interoperability I discussed immediately above.

For example, in the context of any assessment of whether a foreign country's data privacy protection is "essentially equivalent to that guaranteed within the European Union", perhaps it is not necessary to take account of the entire GDPR in every situation? In a general sense, perhaps the administrative layer alluded to above is far less important than is the abuse-prevention layer and the rights layer, and indeed,

---

30 See in particular: J. Palfrey, U. Gasser, *Interop: The Promise and Perils of Highly Interconnected Systems*, Basic Books 2012; and R.H. Weber, "Legal Interoperability as a Tool for Combating Fragmentation" (2014) Global Commission on Internet Governance Paper Series No 4 (Centre for International Governance Innovation).

31 See: D. Svantesson, "The holy trinity of legal fictions undermining the application of law to the global Internet," *International Journal of Law and Information Technology* 2015, vol. 23, no. 3 (2015); pp. 219–234. See further: D. Svantesson, *Solving the Internet Jurisdiction Puzzle*, Oxford 2017, pp. 113–121.

32 J. Palfrey, U. Gasser, *Interop: The Promise*…, p.178.

33 D. Svantesson, *Solving the Internet*…, p. 120.

34 See further: D. Svantesson, "Internet & Jurisdiction Global Status Report 2019", Internet & Jurisdiction Policy Network 2019, Paris, p. 158.

35 See: D. Svantesson, "A 'layered approach' to the extraterritoriality of data privacy laws," *International Data Privacy Law* 2013, no. 3(4); pp. 278–286. See further: D. Svantesson, *Solving the Internet*…, pp. 191–200.

the latter two may be much more palatable to a foreign country pursuing essentially equivalence. At least for those who are open to some form of compromises, this may represent one possible tool for increasing interoperability.

4.5. The problem of "mandate-driven compartmentalisation"

I suspect that a key reason why it often is so difficult to make progress on Internet regulation issues is found in what we may term "mandate-driven compartmentalisation"; that is, while there are many bodies that may develop useful regulatory approaches, they are all working within limited mandates preventing an effective, comprehensive, approach. In this context, it may be noted that the stakeholder survey of the Internet & Jurisdiction Global Status Report 2019[36] – the world's first comprehensive mapping of Internet jurisdiction-related policy trends, actors and initiatives – found that 79% of the surveyed experts do not think there is sufficient international coordination and coherence to address cross-border legal challenges on the Internet.[37]

The regulation of international data transfers is illustrative. Multiple bodies are working on international data transfers. Some do so exclusively from a trade perspective, others from a human rights perspective, yet others focus on law enforcement access to e-evidence etc. However, the problem is that all these issues are interlinked, and we may not be able to find appropriate solutions to any one unless we consider all at once.

4.6. The strong link between security and data privacy

Looking at decisions such as Opinion 1/15, *Schrems I*, and *Schrems II*, as well as cases not discussed above including *Digital Rights Ireland*,[38] *Google Spain*,[39] it is clear that the interest of national security and law enforcement may collide with the right of data privacy. However, it is also clear that those interest may pull in the same direction as data privacy in other instances.[40] In fact, the seemingly ever-increasing threat posed by cybercriminals targeting personal data means that we more and more frequently see clashes where the privacy interests of the suspect must be weighed against the privacy interests of the many victims of the criminal activity targeting personal data. In other words, we find ourselves in a privacy vs. privacy situation in which some privacy

---

36 The Report is based on a large-scale data contribution from 150 key stakeholders from the Internet & Jurisdiction Policy Network from: states, internet companies, technical operators, civil society, academia and international organisations. A full list of the contributing experts is provided in the Report (D. Svantesson, "Internet & Jurisdiction Global Status Report 2019", Paris, Internet & Jurisdiction Policy Network 2019, pp. 9–13).

37 D. Svantesson, "Internet & Jurisdiction Global…, p. 35.

38 Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland & Seitlinger*, ECLI:EU:C:2014:238.

39 Case C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos and Mario Costeja González*, ECLI:EU:C:2014:317.

40 This is discussed in some detail in: Radim Polčák, Dan Svantesson, *Information Sovereignty – Data Privacy, Sovereign Powers and the Rule of Law*, Edward Elgar Publishing 2017.

interests – namely those of the victims – fall on the same side of the equation as does the interest of law enforcement. This is important. However, for anyone seeking solutions relating to international data transfers, there is another observation we can make that is even more significant.

Looking at the decisions mentioned above, it seems to me that we need to approach data privacy, and access to evidence by law enforcement and national security as a package. That is, the concerns about US access to EU personal data discussed in *Schrems II* cannot be overcome merely by focusing on data privacy law alone. Rather, we need to seek solutions that cater for the legitimate needs of law enforcement and national security without data protection being undermined by law enforcement and national security when personal data from the EU enters the US.

The Mutual Legal Assistance (MLA) structure is being improved.[41] Negotiations are in place in relation to improved mechanisms for direct request – across borders – to providers.[42] The Council of Europe's Budapest Convention is being amended by another Additional Protocol.[43] The United Nations Office on Drugs and Crime (UNODC), the United Nations Counter-Terrorism Committee Executive Directorate (CTED) and the International Association of Prosecutors (IAP), have jointly drafted and launched their updated 2021 *Practical Guide for Requesting Electronic Evidence Across Borders*,[44] and there is a forthcoming 2021 *Data Disclosure Framework*[45] that outlines practices developed by international service providers in responding to overseas government requests for data. These are all promising steps that together may create an environment in which it is sufficiently easy for US law enforcement to obtain data from Europe, in a human right respecting manner, for there to be no need for the type of privacy infringements of concern in the *Schrems II* matter.

Of course, I am not so naive as to think this will be an easy journey. Quite the contrary. However, I do think that it is a more plausible path forward than are the alternatives. The EU will not lower the "baseline" set by the Charter, and the US will not simply stop requiring data for law enforcement and national security.

4.7. The need for scalability

In international law, much weight is given to state practice.[46] This ought to create a strong incentive for countries to pursue scalable universal approaches given that a broad uptake of their approaches legitimacies those approaches. However, scalabil-

41 See further: D. Svantesson, "Internet & Jurisdiction Global…, pp. 104–105.

42 For an overview of the issues involved, see: Internet & Jurisdiction Policy Network Toolkit Cross-border Access to Electronic Evidence, 2021.

43 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185, [accessed: 2021.09.09].

44 https://sherloc.unodc.org/cld/en/st/evidence/practical-guide.html [accessed: 2021.09.09].

45 https://sherloc.unodc.org/cld/en/st/evidence/ddf.html [accessed: 2021.09.09].

46 See in particular: art. 38(1)(b) Statute of the International Court of Justice.

ity does not seem to have been considered much in the context of international data transfers.

Rather, states base their approaches solely on domestic law and their needs with the occasional reference to vague principles of international law. *De lege ferenda*, they should also take into account what will be the effect if other countries adopt the same approach;[47] that is the question of scalability.

An illustrative example of the risks associated with ignoring the scalability issue is found in the "rep localisation" requirement found in art. 27 GDPR.[48] Rep localisation requirements mandate that foreign organisation maintain a physical representation in the country imposing the requirement.[49] Thus, organisations cannot access foreign markets without first establishing a physical presence there. This type of requirement has already been adopted into the data privacy laws of countries imitating the GDPR. One example of this is found in the Thai Personal Data Protection Act B.E. 2562 (2019).[50] The obvious question is whether EU-based organisations are going to established representatives in Thailand, and all the other countries that has adopted, and will adopt, rep localisation requirements. I imagine that once every organisation must have a representative in every country in which it has sales, we will see considerable discontent with this unscalable approach.

Where there is a failure to consider scalability, we end up with a widening of the harmful gap between those countries that are dominant in the online environment (typically richer more developed countries) and those that are struggling to reach their potential (typically poorer less developed countries). This is unacceptable.

Elsewhere,[51] I have argued that a scalability assessment is a part of any assessment of proportionality. For clarity and to provide emphasis, I have here rather approached it as a separate matter. The key thing is, of course, to ensure that scalability is considered.

4.8. The many roles of trust

Via the 2019 G20 meeting in Osaka, Japan gained support for the interesting notion of "transborder data flow with trust" earlier articulated at the January 2019 Davos World Economic Forum. In a sense, this concept is uncontroversial. We need transborder data

---

47 Compare to the "global south impact assessment" advocated in D. Svantesson, *Internet & Jurisdiction Global Status Report 2019*, Paris, Internet & Jurisdiction Policy Network 2019, p 64: "it is arguably reasonable to expect lawmakers in those countries that commonly influence policy and law developments globally to conduct what may be termed a 'global south impact assessment', assessing: (1) what impact their approaches will have in the global south, and (2) what will happen if the global south adopts their approaches."

48 For an analysis of art. 27, see further: C. Millard, D. Kamarinou, *Article 27* [in:] *The EU General Data Protection Regulation*, pp. 589–598.

49 See further: D. Svantesson, *Internet & Jurisdiction*…, pp.147–148.

50 Section 37(5).

51 D. Svantesson, "Data localisation trends and challenges: Considerations…, p. 28, http://dx.doi.org/10.1787/7fbaed62-en [accessed: 2021.09.09].

flow, but transborder data flow is only acceptable with trust. In my view, this trust must come in multiple forms. We need to see trust between states. Yet, trust between states is perhaps at a lower level now than it has been for quite some time. We also need trust between states and their citizens. But also this type of trust is low in many countries. In some countries this trust is lacking due to antidemocratic governments. But trust has also decreased in many democratic states as a result of measures imposed due to the pandemic. Furthermore, we need trust between states and companies. Again, this is a form of trust that has decreased over recent years, especially when it comes to the major tech companies. While states used to compete about being the best at accommodating the trendy new tech companies, those same companies are now constantly targeted with criticism. Finally, we need at least one other form of trust; that is, trust between companies and their customers. This form of trust seems to have largely followed the above-mentioned pattern of the trust between trust between states and companies and needs to be restored.

Much work is required to rebuild these forms of trust, and the required work demands a multistakeholder approach. Furthermore, it must be noted that all these forms of trust depend, and must be built on, enforceable legal rights. While many components (business, technical infrastructure etc.) are needed for productive transborder data flow, only adherence to the rule of law in the form of enforceable legal rights can facilitate the trust necessary for the international data transfers on which the world relies today more than ever.

5. Concluding remarks

The regulation of cross-border data flows goes back, at least, to the Swedish Data Act of 1973. Amongst other things, section 11 of that act made clear that:

> If there is reason to assume that personal data will be used for automatic data processing abroad, the data may be disclosed only after permission from the Data Inspection Board [Datainspektionen]. Such permission may be given only if it may be assumed that the disclosure of the data will not involve undue encroachment upon personal privacy.[52]

In other words, this is not a new issue. Yet, while the approach of imposing conditions on international data transfers has long history, the environment in which that approach is being applied has changed dramatically. In this new environment, it is more important than ever that solutions are found that cater for the important forms of international data transfers. As the case law has taught us, such transfers can only

[52] 11 par. Datalag (1973:289) (Swed.). Translation of: "Finns det anledning antaga att personuppgift skall användas för automatisk databehandling i utlandet, får uppgiften lämnas ut endast efter medgivande av Datainspektionen. Sådant medgivande får lämnas endast om det kan antagas att utlämnandet av uppgiften icke kommer att medföra otillbörligt intrång i personlig integritet." The translation was found at http://archive.bild.net/dataprSw.htm (no longer available) and verified by the author.

be accepted where the data subjects are afforded appropriate safeguards, enforceable rights and effective legal remedies.

While speaking of Sweden, I note the Swedish proverb "gör om, gör rätt." ("do it again, do it right"). Perhaps this is rather an apt proverb to guide our future direction in the field of international data transfers.

Literature

Bentzen H., Svantesson D., *Jurisdictional Challenges Related to DNA Data Processing in Transnational Clouds* [in:] *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy*, eds D. Svantesson, D. Kloza, Cambridge–Antwerpia–Portland 2017.

Bygrave L., *International agreements to protect personal data* [in:] *Global Privacy Protection: The First Generation*, eds J. Rule, G. Greenleaf, Cheltenham 2008, revised in 2017, available at SSRN: *https://ssrn.com/abstract=3072270* [accessed 2021.09.09].

Chander A., *Is Data Localization a Solution for Schrems II?*, "Georgetown Law Faculty Publications and Other Works" 2020, 2300, *https://scholarship.law.georgetown.edu/facpub/2300* [accessed: 2021.09.09].

Chander A., Le U., "Data Nationalism", *Emory Law Journal* 2015, vol. 64/3.

Korff D., "Korff on Kuner: *Schrems II* Re-Examined," 3 September 2020, *https://www.ianbrown.tech/2020/09/03/korff-on-kuner-schrems-ii-re-examined/* [accessed: 2021.09.09].

Kuner Ch., "*Schrems II* Re-Examined", Verfassungsblog.de 25 August 2020, *https://verfassungsblog.de/schrems-ii-re-examined/* [accessed: 2021.09.09].

Kuner Ch., "International Agreements, Data Protection, and EU Fundamental Rights on the International State: Opinion 1/15, EU-Canada PNR", *Common Market Law Review* 2018, no. 55.

Mascalzoni D., Bentzen H. *et al.*, "Are Requirements to Deposit Data in Research Repositories Compatible With the European Union's General Data Protection Regulation?", *Annals of Internal Medicine* 2019, no. 170(5).

Palfrey J., Gasser U., *Interop: The Promise and Perils of Highly Interconnected Systems*, New York 2012.

Polčák R., Svantesson D., *Information Sovereignty – Data Privacy, Sovereign Powers and the Rule of Law*, Cheltenham 2017.

Svantesson D., "A 'layered approach' to the extraterritoriality of data privacy laws," *International Data Privacy Law* 2013, no. 3(4).

Svantesson D., "A legal method for solving issues of Internet regulation; applied to the regulation of cross-border privacy issues," *European University Institute Working Paper LAW* 2010, no. 18.

Svantesson D., "Cross-border data transfers after the CJEU's Safe Harbour Decision – A tale of Gordian Knots," *Alternative Law Journal* 2016, no. 41(1).

Svantesson D., "Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines," *OECD Digital Economy Papers* 2020, no. 301, Paris, *http://dx.doi.org/10.1787/7fbaed62-en* [accessed: 2021.09.09].

Svantesson D., "The holy trinity of legal fictions undermining the application of law to the global Internet," *International Journal of Law and Information Technology* 2015, vol. 23, no. 3.

Svantesson D., "What is 'Law', if 'the Law' is Not Something That 'Is'? A Modest Contribution to a Major Question", *Ratio Juris* 2013, no. 26(3), p. 456.

Svantesson D., *Solving the Internet Jurisdiction Puzzle*, Oxford 2017.

The EU General Data Protection Regulation (GDPR): A Commentary, eds Ch. Kuner *et al.*, Oxford 2020.

Trans-Atlantic Data Privacy Relations as a Challenge for Democracy, eds D. Svantesson, D. Kloza, Cambridge–Antwerpia–Portland 2017.

Weber R.H., "Legal Interoperability as a Tool for Combating Fragmentation," *Global Commission on Internet Governance Paper Series Centre for International Governance Innovation* 2014, no 4.

Summary

Dan Jerker B. Svantesson

International Data Transfers post *Schrems* – Moving Towards Solutions

International data transfers are both essential for the modern world and a major source of risks to the protection of personal data. In this, we can speak of a clash between an important multi-faceted objective and the protection of a complex fundamental human right with implications going far beyond that right itself.

The goal must be to facilitate data privacy respecting international data transfers. However, agreement on this goal – even if widespread – does not necessarily signal agreement on how we reach that goal. To make progress, we must proceed with caution and yet avoid getting bogged down in the unavoidable challenges, such as definitional challenges, we will face.

This article canvasses a selection of key considerations that ought to be kept in mind when we discuss approaches to international data transfers. However, to prepare ground for that discussion, it first sets the scene by examining the so-called Schrems II decision, its larger context and background, as well as some of the reactions we have seen to that decision.

Keywords: transfer of data to third country; adequacy; standard contractual clauses; GDPR.

Streszczenie

Dan Jerker B. Svantesson

Międzynarodowy transfer danych po sprawach Schremsa – ku rozwiązaniom

Ponadgraniczny transfer danych jest niezbędny współczesnemu światu, stanowiąc jednocześnie znaczące źródło zagrożeń dla ochrony danych osobowych. W tym kontekście możemy mówić o konflikcie pomiędzy ważnym, wieloaspektowym zadaniem do zrealizowania a ochroną złożonego, podstawowego prawa człowieka, którego skutki wykraczają daleko poza samo prawo.

Celem musi być ułatwienie ochrony prywatności danych przy poszanowaniu potrzeby ponadgranicznego przekazywania danych. Jednak zgoda co do określenia celu – nawet jeśli powszechna – niekoniecznie oznacza porozumienie co do sposobu jego osiągnięcia. Aby poczynić postępy, musimy postępować ostrożnie, a jednocześnie unikać ugrzęźnięcia w gąszczu nieuniknionych wyzwań, z którymi przyjdzie nam się zmierzyć, takich jak choćby wyzwania terminologiczne.

W niniejszym artykule przedstawiono wybrane kluczowe kwestie, o których należy pamiętać, gdy dyskutujemy o naszym podejściu do ponadgranicznego przekazywania danych. Nim ta dyskusja się rozwinie, należy przygotować do niej grunt scenę poprzez zbadanie tzw. orzeczenia *Schrems II*, jego szerszego kontekstu, tła, a także niektórych reakcji, z jakimi mieliśmy do czynienia w związku z tym orzeczeniem.

Słowa kluczowe: transfer danych do państw trzecich; adekwatność; standardowe klauzule umowne; RODO.