The implications of the Schrems judgment of the European Court for data transfers to the U.S.

Prof. Lokke Moerel

In the Schrems judgment the Court of Justice of the European Union (CJEU) invalidates the EU-US Safe Harbor Framework for data transfers to the US, but does this judgement also have consequences for the alternative data transfer instruments, like the EU Standard Contractual Clauses (SCCs) and so-called Binding Corporate Rules (BCR)? Are data transfers to other countries outside the EU like China and India now also at risk? Does the new EU-US Privacy Shield agreement solve the data transfer issues to the US?

1. Summary findings

The Schrems judgment relates to an ‘adequacy decision’ of the European Commission based on Article 25 of the European Privacy Directive (Directive). These adequacy decisions are of a completely different nature than the decisions of the Commission or national Data Protection Authorities (DPAs) based on Article 26 Directive, authorizing alternative data transfer instruments, such as SCCs and BCR. In the first case, the Commission evaluates whether the legal regime of the country of destination is adequate, as a result whereof data transfers can take place without implementing additional contractual safeguards. In the second case, the Commission or national DPA evaluates whether a set of contractual measures/BCR provide for sufficient safeguards in case the legal regime of the country of destination is not adequate. These two assessments: (1) whether the law is adequate or (2) whether contractual measures can provide sufficient safeguards when the law is not adequate, are different assessments based on different criteria. For assessment (2), the assessment of the adequacy of US law in the Schrems case (assessment (1)), is therefore not relevant. The adequacy of the laws of the country of destination is one factor only for the assessment whether contractual measures can provide adequate safeguards. Any other interpretation would lead to the current system of derogations for data transfers to non-adequate countries under the Directive and the upcoming European General Data Protection Regulation (GDPR) having no function. Transfers would then only be possible to countries providing an adequate protection, which is contrary to the legislative history of the Directive and the GDPR.

The Schrems judgment further confirms that only the CJEU - and not national DPAs or courts - can strike down a decision of the Commission authorizing SCCs under Article 26 Directive. As a consequence, the SCCs (and BCR) remain valid. Recent blanket statements by certain national

1 Lokke Moerel is Senior of Counsel Morrison & Foerster, Berlin and Professor of Global ICT Law at Tilburg
DPAs that these transfer instruments are no longer valid for data transfers to the US are therefore legally unfounded.

National DPAs remain, however, at all times authorized, when hearing a claim, to examine the relevant specific data transfers. This requires a case-by-case assessment considering all relevant circumstances. The 'adequacy' of the laws of the country of destination is again one factor only and can in itself not be the basis for deciding that the transfers under SCCs or BCR should be prohibited or suspended. This applies also to the CJEU when it would be requested to decide whether SCCs and BCR constitute valid instruments for transfers to the US.

The EU data transfer rules are further based on the fundamental starting point that data transfers may take place to countries that provide a level of protection of fundamental rights that is essentially equivalent to that guaranteed in the EU legal order. It is therefore not appropriate to hold the US to higher standards than we live up to ourselves. Similar concerns could further be raised in respect of the surveillance powers and redress mechanisms in many other countries outside the EU, including other major trading partners of the EU, such as China, Russia, Japan, South Korea, India, Brazil and Canada. Applying inconsistent and discriminatory rules would likely violate the EU's international trade commitments.

2. Background

On 6 October 2015, the CJEU issued its judgment in the case between Max Schrems and Facebook (Schrems judgment).2 Schrems had requested the Irish Data Protection Authority (Irish DPA) to investigate the level of protection of European personal data after these have been transferred to the US. According to Schrems, the Snowden disclosures showed that the US violated the privacy of European citizens after their data were transferred by Facebook to the US. The case was referred to the CJEU, which invalidated Decision 520/2000/EC of the European Commission (Commission), that approved the Safe Harbor regime as providing for an adequate level of protection of personal data when assessed against the standard set by EU data protection law (Safe Harbor Decision), which was the legal basis for the data transfers of Facebook from the EU to the US.

Since 2000, European companies could transfer personal data to US companies that adhered to the Safe Harbor Framework, and were considered ‘safe’ for the transfer of data based on the Safe Harbor Decision by the Commission. About 4,000 companies were Safe Harbor certified, among which many providers of cloud services. As a result of the Schrems judgment, these transfers were invalidated as the privacy of European citizens was not considered being adequately protected. The CJEU based its decision also on an evaluation of the Safe Harbor Framework performed by the Commission itself, which concluded that the powers of the US authorities went beyond what was strictly necessary and proportionate to the protection of national security and that individuals did not have adequate means of judicial redress to protect their privacy. These concerns equally apply

2 C-362/14 Schrems ECLI:EU:C:2015:650
when data are transferred to the US based on other data transfer instruments, such as the SCCs and BCR.

The concern that the intelligence services of certain countries have too broad surveillance powers and citizens do not have adequate redress mechanisms to protect their privacy in respect thereof, equally applies to other important trading partners of the EU, such as China, Brazil, and India to name a few. The EU has not entered into data transfer agreements with these countries, and these are also not expected in the coming time. If the alternative transfer instruments are no longer valid, this would make trade between the EU and these countries very difficult.

The concern that in certain countries the intelligence services have too broad surveillance powers is a legitimate concern. This concern, however, (by now) also applies to some of the EU member states themselves. More in general, it seems a fair statement that currently in the EU there does not seem to be uniform consensus on what the scope is of the "national security exemption" in Article 8 of the European Charter of Human Rights. More clarity may come from three cases pending before the European Court of Human Rights, which are instigated by the UK Bureau of Investigative Journalism and a number of civil rights organizations, and claim that the generic surveillance powers of the UK intelligence services violate Article 8 of the European Convention of Human Rights.

This is relevant, as the EU data transfer rules are based on the fundamental starting point that data transfers may take place to countries that provide a level of protection of fundamental rights that is essentially equivalent to that guaranteed in the EU legal order. As a result, DPAs deciding on a claim that transfers under SCCs or BCR are in violation of the Directive, have to establish whether in the relevant specific circumstances of the case, the law of the importing country goes beyond “what is necessary in a democratic society”, in order to establish “equivalency”.

It is clear that the discussion when to allow data transfers between countries based on the respective surveillance powers judicial redress available to citizens should be addressed at the political level between these countries. Invalidating data transfer mechanisms which govern data transfers between private companies puts these companies in an impossible position. If the US authorities issue a subpoena to a US group company (or its US cloud provider), the company has the option to ignore a validly issued subpoena or to violate EU data protection rules. This is

---

3 See reports in n 29.

4 This is also the conclusion of the EU current state of affairs by the European Union Agency for Fundamental Rights (FRA), in its report of November 2015, 'Surveillance by Intelligence Services: Fundamental Rights, Safeguards and Remedies in the EU, mapping Member States' legal frameworks'; the FRA further concludes that judicial remedies against EU intelligence services suffer from some of the same problems identified in respect of redress by EU citizens against the US intelligence services in the US.

5 Bureau of Investigative Journalism and Alice Ross vs. the United Kingdom, App. No. 62322/14, lodged on 11 September 2014; Joint application under Article 34, Big Brother Watch, Open Rights Group, English PEN, Dr. Constanze Kurz v. the United Kingdom, App. No. 58170/13; The American Civil Liberties Union, Amnesty International, Bytes for All, the Canadian Civil Liberties Association, the Egyptian Initiative for Personal Rights, the Hungarian Civil Liberties Union, the Irish Council for Civil Liberties, the Legal Resources Centre, Liberty, Privacy International) v. UK, App. No. 24960/15.

Prof. dr. Lokke Moerel
passing the “hot potato” to parties that cannot influence nor control the outcome of the negotiations on privacy by EU and US authorities.

Following the Schrems judgment, the WP29 encouraged US and EU authorities to complete ongoing negotiations and develop a revised and improved Safe Harbor Framework to satisfy EU privacy rules. It warned that failure to reach an appropriate solution by late January 2016 could lead individual DPAs to step in and protect individuals by exercising their authority to conduct coordinated enforcement actions and suspending individual transfers. The WP29 also urged current Safe Harbor organizations to implement temporary measures, such as SCCs or BCR, ensuring continued compliance with EU data transfer rules. In order to legitimize their data transfers, these companies put in place alternative data transfer mechanisms, such as the SCCs and BCR.

In the meantime, the Commission and the US announced that they have reached an agreement on a Safe Harbor 2.0, re-labelled as the ‘EU-U.S. Privacy Shield’ (Privacy Shield). The Privacy Shield was officially adopted on 12 July 2016. The approval came only a few months after the EU and US released an initial draft of the Privacy Shield, on 29 February 2016, which had been criticized by civil rights organizations, the European Parliament, the WP29 and the European Data Protection Supervisor (EDPS) that the terms do not yet meet the requirements set by the CJEU. Despite such criticism, amendments to the February draft are minimal. This being said, it is the first time that the US government commits itself to restrict the general surveillance of data of EU citizens and to provide individuals with redress against the US intelligence services before a US ombudsman. The US undertakings further extend the Privacy Shield surveillance commitments to all EU personal information transfers, regardless of the data transfer instrument used. In a statement issued on 26 July 2016, the WP29 remains critical of some aspects of the finalized Privacy Shield. However, WP29 will not further pursue these concerns for now, but rather use the

---


12 Privacy Shield Documentation, n 7, in particular Annex III.

13 The privacy Shield Documentation explicitly states that those safeguards apply to all EU personal information transferred to the US for commercial purposes, see Privacy Shield Documentation, n 7, Communication, section 3.2, p. 10.
first annual review of the Privacy Shield for further evaluation. The WP29 also explicitly refers to the first annual review to evaluate the impact of U.S. public authorities’ access to personal information on other transfer tools, such as SCCs and BCR.

In related developments, the Hamburg DPA, stated in a recent trade press interview that he is hoping that new legislation under development in Germany will make it possible for the country's DPAs to challenge EU adequacy decisions as soon as next year. He is quoted as saying that he has “serious doubts whether [the Commission’s] adequacy decision meets the legal requirements of the principle of proportionality and judicial redress in the [ECJ] Safe Harbor decision.” In April 2016, the Bundesrat, Germany's legislative body which represents the sixteen Länder (federal states) of Germany at the national level, asked the government to make it possible for federal and state DPAs to challenge the European Commission's adequacy decisions by allowing the DPAs to go directly to a national court to request a referral to the ECJ (a right which they currently do not have). In mid-July, the government responded to the Bundesrat and said that it is working on the new legislation but did not indicate if it would allow DPAs to challenge EU adequacy decisions.

As a final development, it should be mentioned that after the Schrems judgement, the case was referred to the Irish High Court which, in its turn, referred the case back to the Irish DPA to investigate whether, in the absence of Safe Harbor Decisions, Facebook has valid grounds for data transfers to the US. The Irish DPA has now issued a draft decision with the initial finding that the SCCs are not a valid basis for transfers to the US, mainly because of the lack of effective redress in the US when personal data are processed by US government agencies for national security purposes. As the Irish DPA is not authorized to declare the SCCs invalid itself (only the CJEU can do this), the Irish DPA has decided to initiate immediate legal proceedings with the Irish national court whether it agrees with this initial finding and subsequently request a ruling of the CJEU on the validity of the Commission's decisions approving the SCCs (SCCs Decisions). The Irish DPA maintains that it cannot conclude its investigation without obtaining a ruling from the CJEU on the validity of the SCCs Decisions. The whole procedure will probably take at least two years, considering the fact that the Schrems judgment took the CJEU already 15 months to decide after the matter had been referred to it by the Irish High Court. In the meantime, the Irish DPA continues its investigation into the contractual arrangements in place between Facebook Ireland and Facebook US and between Facebook US and third party sub-processors as well as the adequacy of the protection provided by the US. The data transfers of Facebook under the SCCs are therefore currently not suspended.

Below I will discuss what the effects of the Schrems case are on the alternative data transfer mechanisms and whether the Irish DPA is right in finding that the SCCs are invalid because of the lack of redress in the US.

---


15 This draft decision has not been published, but has been provided to me for review.

Prof. dr. Lokke Moerel
Before answering these questions, I will first describe the EU data transfers rules in more detail. In par. 4, I will then discuss the Schrems judgment, after which I will discuss in par. 5 the impact of this judgment on the alternative data transfer instruments, such as the SCCs as approved by the Commission or BCR, to facilitate intra-group data transfers. I will further discuss the merits and potential impact of the draft-decision of the Irish DPA, according to which the SCCs should also be declared invalid for data transfers to the US. I will end with a summary conclusion.

3. The EU data transfer regime

The general rule under the Directive is that personal data can only be exported by a company established in the EU to third countries that provide an “adequate level of protection” for such data, unless certain conditions have been met (Article 25(1) of the Directive). Those conditions are split into two categories.

3.1. Transfers based on an “adequacy decision” (issued under Article 25(6) of the Directive): Article 25(6) of the Directive allows the Commission to find – via an “adequacy decision” – that certain legal regimes are ‘adequate’ when assessed against the standard set by EU data protection law. Specific jurisdictional adequacy decisions include those permitting data export to Canada, New Zealand and Israel. Only a very limited number of countries have obtained an adequacy decision, and these do not include the main trading partners of the EU, such as China, Japan, Russia, India, and Brazil. The procedure for countries to obtain an adequacy decision can take years and requires a full assessment by the Commission of the rule of law, access to justice as well as international human rights, norms and standards in such country, which assessment further has to be revised on a regular basis. As a consequence, this transfer ground has proven of limited practical value.

3.2. Specific data transfers grounds (regulated under Article 26 of the Directive): the general rule that personal data may only be exported from the EU to third countries that provide an “adequate level of protection” for such personal data is subject to a number of explicit “derogations”. These derogations are set forth in Article 26 of the Directive, listing the circumstances in which a data exporter is permitted to transfer personal data from the EU to a data importer in a jurisdiction that does not, or has not been recognized to provide an ‘adequate’ level of protection as determined under EU data protection law. The specific derogations provided by Article 26 of the Directive can (in their turn) be split into two categories:

3.2.1. Specific legal basis provided by Article 26(1) of the Directive: such as (a) where the individual has given consent for the transfer; when the transfer is (b) necessary in relation to a contract (‘contractual necessity’) or (c) a legal claim; (d) necessary or legally required on important public interest grounds; or (e) necessary in order to protect the vital interests

---

16 Currently, adequacy decisions have been adopted with regard to the following countries: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay. See: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

17 Schrems, para. 76.
of the data subject. These derogations are also included in the GDPR (and even extended),\textsuperscript{18} which supports the conclusion that this system is not under discussion.

As to the legal basis of consent, it should be noted that EU data protection law expressly recognizes that consent is a core part of the right to data protection. The consent-derogation is based on the essential premise that a data subject is aware of the risks that he or she is assuming by permitting the export of their personal data outside the EEA to the specified data importer, but chooses to act regardless of having been informed of the transfer.\textsuperscript{19} This is in line with Article 8 of the Charter of Fundamental Rights, which expressly recognizes that consent is a core part of the right to data protection.\textsuperscript{20} Consent is an important safeguard which respects data subjects’ autonomy, allowing individuals to control the access to and collection of their information.\textsuperscript{21} Also the “contractual necessity”-basis is based on the premise that a data subject is aware of the risks that he or she is assuming by entering into a transaction where it is necessary for their personal data to be exported outside Europe.\textsuperscript{22} In other words, data subjects are free to determine whether or not they enter into contracts that would inherently require the transfer of their data outside the EU, also if this would imply that their privacy will be violated.

\textbf{3.2.2. The controller “adduces adequate safeguards” pursuant to Article 26(2) of the Directive:} the Directive explicitly envisages that the data exporter and data importer may also agree to safeguards specifically for their transfer, in particular in the form of contractual clauses. Article 26(2) allows Member States to authorize transfers to a non-adequate country:

\textsuperscript{18} See Chapter V of Regulation (EU) No. 679/2016 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (\textit{General Data Protection Regulation}): \url{http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN}. Article 49(1) GDPR provides for an additional ground: a data transfer may, under limited circumstances, be justified on a legitimate interest of the controller or processor.

\textsuperscript{19} This is expressly stated as the intention behind Article 26(1) in the travaux préparatoires – see COM(92) 422 final - SYN 287 at page 35.

\textsuperscript{20} Article 8(2) of the Charter explicitly recognises that the ability of data subjects to consent (or not) to how their data are used is a primary aspect of the right to the protection of personal data: “data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law” (\textit{emphasis added}).

\textsuperscript{21} See by analogy, \textit{Vereniging Rechtswinkels Utrecht v Netherlands 46 DR 1986, EcomHR}, where applicant argued that the termination of an agreement whereby complainant received access to a prison for purposes of providing legal counsel to prisoners for reasons of giving statements in the press constituted a violation of his freedom of speech. The European Commission of Human Rights (at the time the gatekeeper for access to the European Court of Human Rights) ruled that the applicant had the right to make statements in the press, but that these were in violation of the contractual terms, and therefore the contract was validly terminated. In other words, Article 10 European Convention of Human Rights (ECHR) is not violated if an individual gives permission or agrees to contractual terms which restrict his freedom of expression. See also, by analogy, the case of \textit{Stedman v UK (1997) 23 EHR CD168} where the applicant complained that her dismissal due to her refusal to work on Sundays was an interference with her religious freedoms. The European Commission of Human Rights held that the applicant was dismissed because she refused to work regular working hours and not because of her religion. She had a free choice in employment, could have taken another job and thus the right of freedom of religion was not engaged.

\textsuperscript{22} This is expressly stated as the intention behind Article 26(1) in the travaux préparatoires – see footnote 11.
“where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights” whereby “such safeguards may in particular result from appropriate contractual clauses” (bold added)

Since 2001, the Commission adopted a number of decisions under Article 26(4) approving standard contractual clauses for the transfer of data to processors and controllers in third countries (the “SCCs Decisions”). Controllers and processors can also “adduce appropriate safeguards” under Article 26(2) for their intra-group transfers by adopting ‘binding corporate rules’ (BCR). As BCR are not codified in the Directive, BCR are subject to national authorization by the national DPAs. Since 2003, the Working Party 29 (WP29) has adopted a series of Working Documents, setting out the criteria that the WP29 recommends being incorporated in BCR and considered by the national DPAs in their assessment of adequacy. The GDPR now explicitly includes BCR as a data transfer tool and codifies the criteria set out by the WP29. To provide more flexibility for companies, the GDPR adds, as new components, that appropriate safeguards may also be provided for by approved codes of conduct and certification mechanisms, as well as standard data protection clauses adopted by a DPA and declared generally valid by the Commission.

Compared to ‘adequacy decisions’ which result from the overall assessment of a given third country's legal system and which in principle may cover all transfers to that country, the alternative bases for transfers under Article 26 have both a more limited scope (as they apply only to specific data flows) and a broader coverage (as they are not necessarily confined to a specific country). They apply to data flows carried out by particular entities which have decided to make use of one of the possibilities offered by Article 26 of the Directive.

4. The main findings of the Schrems judgment

In the Schrems judgment, the CJEU invalidated Decision 2000/520/EC of the European Commission (Commission) which approved the Safe Harbor regime as providing for an adequate level of protection of personal data when assessed against the standard set by EU data protection law (Safe Harbor Decision).


25 Article 46(2)(b) and 47 GDPR.

26 Article 46(2) GDPR.

27 See in these words in Commission Communication, p. 5.
The CJEU found that, in order for the Commission to adopt a decision pursuant to Article 25(6) of the Directive, it must find, duly stating reasons, that the third country concerned in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights that is essentially equivalent to that guaranteed in the EU legal order (known as an ‘adequacy decision’).

The CJEU held that the Commission’s Safe Harbor Decision did not state that the US in fact ‘ensures’ an adequate level of protection (Schrems para 97). For this conclusion the CJEU considers relevant that:

- the Safe Harbor Decision “does not contain any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data are transferred from the European Union to the United States (Schrems para. 88);

- nor does refer to the existence of effective legal protection against interference of that kind” (Schrems para. 88);

- the Safe Harbor Decision itself explicitly provides28 that the safe Harbor principles can be restricted insofar as necessary for ‘national security, public interest, or law enforcement requirements’ (Schrems para. 84);

- the Commission itself has established in its earlier evaluation of the Safe Harbor Framework29 that (i) the powers of the United States authorities went beyond what was strictly necessary and proportionate to the protection of national security; and (ii) that the data subjects “had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased” (Schrems para. 90).

The CJEU further held that Commission decisions, such as the Safe Harbor Decision, are binding upon the Member States, and can only be invalidated by the CJEU (Schrems para. 51-52). However, such a binding decision does not prevent the national DPAs, when hearing a claim lodged by a person concerning his or her data protection rights, to examine such claim with powers conferred upon the DPAs under Article 28 of the Directive, with complete independence, whether the relevant transfer of that data complies with the requirements laid down by the Directive (Schrems para. 57). The CJEU held that the Safe Harbor Decision denied the national DPAs such powers under Article 28 of the Directive (Schrems para 102).

The CJEU then declared the Safe Harbor Decision invalid: “without there being any need to examine the content of the Safe Harbor principles” (Schrems para. 98).

---

28 See fourth paragraph of Annex I.
The CJEU referred the case back to the Irish High Court which, in its turn, referred the case back to the Irish DPA to investigate whether, in the absence of Safe Harbor Decisions, Facebook has valid grounds for data transfers to the US. The Irish DPA has now issued a draft decision that questions the validity also of the use of the SCCs for transfers to the US because of the lack of effective redress in the US when personal data are processed by US government agencies for national security purposes. The Irish DPA has decided to initiate immediate legal proceedings with the Irish national court on the basis of its initial findings so that the national court can determine whether to request a ruling of the CJEU on the validity of the Commission's decisions approving the SCCs (SCCs Decisions). The Irish DPA maintains that it cannot conclude its investigation without obtaining a ruling from the CJEU on the validity of the SCCs Decisions. The whole procedure will probably take at least two years, considering the fact that the Schrems judgment took the CJEU already 15 months to decide after the matter had been referred to it by the Irish High Court. In the meantime, the Irish DPA continues its investigation into the contractual arrangements in place between Facebook Ireland and Facebook US and between Facebook US and third party sub-processors as well as the adequacy of the protection provided by the US. The data transfers of Facebook under the SCCs are therefore currently not suspended.

Noteworthy is that the CJEU did not independently assess whether the Safe Harbor principles provide for an adequate level of protection. The CJEU based its ruling on a conclusion of law that the Commission’s findings in the Safe Harbor Decision itself are inadequate, also in light of the Commission’s own later findings in its evaluation of the Safe Harbor Framework. These findings date from 2013 and, since then, more in-depth research has been undertaken into the adequacy of US law, the US government access powers to data of European citizens and the safeguards provided to EU citizens in respect thereof as well as into government access powers in the EU and safeguards provided to EU individuals in respect thereof, in order to establish equivalence. In particular, I refer to the opinion of Geoffrey Robertson QC, of December 4, 2015, evaluating European standards of privacy protection compared to the US. It should further be pointed out that, since 2013, the US has undertaken substantive reforms of its legal regime because of, and

---

30 See n 15.
31 See e.g. European Union Agency for Fundamental Rights, Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU, mapping Member States’ legal frameworks, November 2015; the Sidley Austin report, “Essentially Equivalent, A comparison of the legal orders for privacy and data protection in the European Union and the United States, January 2016, to be found at http://www.sidley.com/-/media/publications/essentially-equivalent--final.pdf. This report was commissioned by the U.S. Chamber of Commerce, The Software Alliance, the Computer and Communications Industry Association, and the Information Technology Industry Council and provides a comprehensive comparison of US and EU legal frameworks, particularly with respect to government access to data for law-enforcement and intelligence purposes. The report compares the EU and US legal orders on government surveillance, which were central to the allegations influencing Mr. Schrems’ complaint in Ireland. To assess the EU legal order, the report focuses on the laws in eight EU Member States (Belgium, France, Germany, Ireland, Italy, the Netherlands, Poland, and the UK). See further: Privacy and Civil Liberties Oversight Board: Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, July 2, 2014, see also the President’s Review Group on Intelligence and Communications Technologies, Report and Recommendations of The President’s Review Group on Intelligence and Communications Technologies (12 Dec 2013) available at: https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf; and Professor Peter Swire: US Surveillance Law, Safe Harbor, and Reforms, December 17, 2015.
consequent upon, the Snowden revelations. Based on this research and legal developments, the conclusions of the Commission from 2013 are no longer current and merit (a more in-depth) re-assessment. Further, the conclusions of the Schrems judgment relating to the Safe Harbor Decision have no relevance for the Privacy Shield. This memorandum does not take into account, and therefore does not contain, any views on the adequacy of the terms of the new Privacy Shield.

5. **Impact of the Schrems judgment on EU data transfer grounds**

Looking at the data transfer grounds discussed in paragraph 3, the Schrems decision has the following consequences.

5.1. **‘adequacy decisions’ (Article 25 of the Directive)**

The Safe Harbor Decision concerns an ‘adequacy decision’ under Article 25 of the Directive. The Schrems judgment focused only on the Safe Harbor Decision and whether it was an appropriate adequacy decision under Article 25. The Schrems judgment will likely impact other adequacy decisions under Article 25(6) because these also deny the national DPAs the powers which they derive from Article 28 of the Directive. Confirming this view, the Commission stated that Article 25(6) decisions may need to be amended following the Schrems judgment.33

5.2. **Specific data transfers grounds (Article 26 of the Directive)**

In contrast, the derogations in Article 26 of the Directive are intended to allow transfers to jurisdictions that do not provide for adequate protection. The CJEU in the Schrems decision did not opine on the appropriateness of the derogations in Article 26. Following the Schrems decision, the Commission stated that the derogations in Article 26 remain valid.34 Moreover, the derogations listed in Article 26 have all been maintained in the adopted text of the General Data Protection Regulation (GDPR),35 demonstrating their continued relevance and validity. Far from reducing reliance on the derogations, the GDPR substantially extends the derogations in Article 26,

---

33 “The scope of the judgment is limited to the Commission’s Safe Harbor Decision. However, each of the other adequacy decisions contains a limitation on the powers of the DPAs that is identical to Article 3 of the Safe Harbor Decision and which the Court of Justice considered invalid. The Commission will now draw the necessary consequences from the judgment by shortly preparing a decision, to be adopted pursuant to the applicable comitology procedure, replacing that provision in all existing adequacy decisions.” Communication on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment of the Court of Justice in Case C-362/14 (Schrems) COM (2015) 566 Final, 6 November 2015 (the “Commission Communication”), pages 14 and 15.

34 Commission Communication, p. 15.

35 See Chapter V of the GDPR.
recognizing that the current transfer rules constitute substantial impediments to trade\textsuperscript{36} and the limited value of the ‘adequacy system’ in practice for companies.\textsuperscript{37}

The legislative intent to permit transfers to countries that are not adequate is also set forth in the text of Article 26 of the Directive itself. Article 26(1) expressly provides that its operation is “by way of derogation from Article 25” and that EU Member States’ data protection law “shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2) may take place on condition that …” (emphasis added).

It is important to establish that the \textit{Schrems} judgment has no relevance for the validity of the derogations provided for by Article 26(1) of the Directive, such as consent and contractual necessity. Article 26(1) is designed to set up a framework to allow the transfer of personal data in specific cases where the EU regulators determined that certain transfers should be permitted regardless of the lack of adequacy in the regime of the data importer (for example, where the data subject him/herself has exercised choice (consenting to the transfer), where there are circumstances necessitating the transfer (performance of a contract), or in circumstances of important public interest or the vital interest of the individual). Those determinations are entirely separate from the analysis of adequacy. By definition, the failure of the Commission to properly assess adequacy in the Safe Harbor context should therefore have no bearing on whether the derogations under Article 26 are appropriate. Following the \textit{Schrems} judgment, the Commission therefore stated that the derogations in Article 26(1) remain valid:

“In the absence of an adequacy decision under Article 25(6) of Directive 95/46/EC and irrespective of the use of SCCs and/or BCRs, personal data may still be transferred to entities established in a third country to the extent that one of the alternative derogations set out in Article 26(1) of Directive 95/46/EC applies;”\textsuperscript{38}

and

“These grounds provide a derogation from the general prohibition of transferring personal data to entities established in a third country without an adequate level of protection. In fact, the data exporter does not have to ensure that the data importer will provide adequate protection, and he will usually not need to obtain prior authorisation for the transfer from the relevant national authorities.”\textsuperscript{39}

\textsuperscript{36} See Chapter 2 of the Explanatory Memorandum of the Commission to the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM/2012/011 final - 2012/0011 (COD), to be found at: \url{http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&qid=1464772527190&from=EN}.

\textsuperscript{37} See WP169 ‘The Future of Privacy’, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, 1 December 2009, p. 2 and 11.

\textsuperscript{38} Commission Communication, para. 2.3.

\textsuperscript{39} Commission Communication, p. 9.
However, as held by the CJEU (Schrems para. 57), the national DPAs remain authorized, when hearing a claim lodged by a person concerning his or her data protection rights, to examine, whether the relevant transfer of that data complies with the requirements laid down by the Directive. Such investigation will, however, be restricted to examining whether the requirements for the relevant legal basis are met, e.g., whether consent in the specific case is ‘freely’ given or whether ‘contractual necessity’ exists. In these evaluations, the ‘adequacy’ of the regime of the data importer is not relevant.

5.3. The controller “adduces adequate safeguards” pursuant to Article 26(2) of the Directive

Controllers can ‘adduce adequate safeguards’ pursuant to Article 26(2) by entering into Standard Contractual Clauses for the transfer of data to processors and controllers in third countries (SCCs) or by adopting Binding Corporate Rules (BCR).

SCCs

The SCCs derive from decisions of the Commission. They are EU legal measures which are binding upon all Member States (including national institutions such as DPAs). Commission decisions, such as the SCCs Decisions, must also be presumed to be lawful, in accordance with well-established principles of EU law. This presumption of legality was expressly reiterated by the CJEU in the Schrems judgment.

As noted above, only the CJEU – not national regulators or courts – can strike down the SCCs Decisions. Until such a time (if any) as this occurs, the SCCs Decisions are binding on national courts and DPAs.

On 6 November 2015, the European Commission reiterated this position:

“Since Commission decisions are binding in their entirety in the Member States, incorporating the SCCs in a contract means that national authorities are in principle under the obligation to accept those clauses. Consequently, they may not refuse the transfer of data to a third country on the sole basis that these SCCs do not offer sufficient safeguards.” (emphasis added)

However, as held by the CJEU (Schrems, para. 57), it remains the case that national DPAs are authorized, when hearing a claim, to examine whether a specific data transfer under SCCs

---

40 See footnote above.
41 Article 288 of the TFEU provides that “A decision shall be binding in its entirety. A decision which specifies those to whom it is addressed shall be binding only on them.” The SCC Decision is addressed to all Member States.
42 See Case C-475/01 Commission v Greece paragraph 18; Case C-137/92 P Commission v BASF and Others paragraph 48; and Case C-245/92 P Chemie Linz v Commission paragraph 93.
43 Schrems paragraph 51: “Measures of the EU institutions are in principle presumed to be lawful and accordingly produce legal effects until such time as they are withdrawn, annulled… or declared invalid”.
44 Schrems, paragraph 61.
45 Commission Communication, p. 6.
complies with the requirements laid down by the Directive. This competence of the DPAs is duly reflected in the SCCs themselves, where Article 4 of the SCCs provides that the DPAs may exercise their powers to suspend or prohibit data flows in cases where:

“the law to which the data importer or a sub-processor is subject imposes upon him requirements to derogate from the applicable data protection law which go beyond the restrictions necessary in a democratic society […], where those requirements are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses” (emphasis added).46

The test to be applied here by the individual DPAs under Article 4 of the SCCs is very different from the assessment to be made by the Commission to decide on an adequacy decision (and as evaluated in the Schrems judgment). First of all, the Commission has already made an assessment in respect of the SCCs that these do adduce adequate contractual safeguards under Article 26(4) of the Directive. Note also that the function of the SCCs Decisions by the Commission under Article 26(4) of the Directive is already very different from an ‘adequacy decision’. In the latter case the Commission evaluates whether the laws of a country provide for adequate safeguards so transfers can take place without any additional mitigating (including contractual) measures. Under the SCCs Decisions, the Commission evaluates whether a certain set of contractual clauses will offer sufficient safeguards so transfers can take place to a country that does not provide for adequate protection. These two assessments: (1) whether the law is adequate or (2) whether contractual measures can provide sufficient safeguards if the law is not adequate, are entirely different assessments based on different criteria. For assessment (2), the Schrems judgment is not relevant.

Commission’s decisions are further binding upon the Member States and the DPAs and the SCCs Decisions are assumed to be valid, which in this case means that the DPAs will have to take as a given that the SCCs in principle provide for adequate contractual safeguards. A national DPA may subsequently prohibit or suspend a transfer on the basis of Article 4(1)(a) of the SCC Decision. In such case, the DPA will need to investigate whether, in the relevant specific circumstances of the case, the relevant data transfers have such a substantial adverse effect on the individuals. Relevant factors will include:

46 See the full text of Clause 4(1)(a) SCCs under Decision 2010/87/EU:
“Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to Chapters II, III, V and VI of Directive 95/46/EC, the competent authorities in the Member States may exercise their existing powers to prohibit or suspend data flows to third countries in order to protect individuals with regard to the processing of their personal data in cases where:

(a) it is established that the law to which the data importer or a sub-processor is subject imposes upon him requirements to derogate from the applicable data protection law which go beyond the restrictions necessary in a democratic society as provided for in Article 13 of Directive 95/46/EC where those requirements are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses.”

47 Whether or not ultimately an adequate level of protection is in place “should be assessed in the light of all the circumstances surrounding the data transfer operation”. Recital 3 of the SCC Decision.

Prof. dr. Lokke Moerel
• the nature of the data transferred (are the data sensitive in nature and/or of interest to US governmental agencies to start with?);

• the purpose of the transfer (is this of added value to the individuals concerned?);

• the amount and type of subpoena’s received by the data importer in the past (are these excessive in number or limited, do these concern specific investigations into e.g. fraud or are these of a generic nature, e.g. bulk tapping?);

• specific additional mitigating measures implemented by the data exporter and importer (e.g., are the data encrypted in such a manner that the US authorities will not be able to decrypt?).

Such factors will have to be assessed in light of the contractual safeguards adduced by the SCCs (see examples below). The DPA will further have to conduct its own assessment into the current state of the relevant law and practice in the destination country. By now that will include any safeguards provided for by Privacy Shield, as these also apply to transfers under SCCs (and BCR).\(^{48}\)

It is clear, therefore, that this is a much more stringent test than the test to assess whether the laws of a country are adequate. This test requires a case-by case assessment by the DPA upon hearing a claim in respect of a specific transfer, as to whether in the specific circumstances of the case, such substantial adverse effect on the individuals concerned is likely. DPAs which are requested to assess specific data transfers under SCCs can therefore not prohibit or suspend transfers on the sole consideration that the system of a country is not considered adequate for reasons of too extensive government access and lack of redress for individuals (as the CJEU did in the Schrems judgment). It is therefore possible that the laws of a country will not be considered adequate for reasons of too extensive government access powers and lack of redress for individuals, while specific transfers under the SCCs are allowed to such country. As noted previously, the SCCs are intended to facilitate transfers to countries whose systems are not considered adequate. Any other interpretation would lead to the current systems of derogations for data transfers to non-adequate countries under the Directive having no function. Transfers would then only be possible to countries providing an adequate protection, which is contrary to the legislative history of the Directive which recognizes that data transfers to third countries are an intrinsic part of trade and that data exporters and data importers should be able to adduce adequate safeguards despite the fact that these third countries are not considered adequate.

Recent blanket statements by certain national DPAs that the SCCs do not constitute valid instruments for data transfers to the US are therefore legally unfounded. This is not for the national DPAs or the WP29 to decide. At the most, the WP29 can issue guidelines for the national DPAs to evaluate data transfers under SCCs in case of complaints. Possible is also that the WP29 issues recommendations to the Commission on how to improve the SCCs.

\(^{48}\) See n 13.
The next question is what the CJEU would likely decide when requested to declare the SCCs invalid for data transfers to the US. Here again, I refer to the fact that compared to ‘adequacy decisions’ which result from the overall assessment of a given third country's system and which in principle may cover all transfers to that system, the alternative bases for transfers like the SCCs have a broader coverage as they are not necessarily confined to a specific country. They apply to data flows carried out by particular entities which have decided to make use of one of the possibilities offered by Article 26 of the Directive. In that light, it is unlikely that the CJEU would invalidate the SCCs integrally. Again, the SCCs may well prove sufficient, dependent on the specific transfer. The most simple example is where the data exporter and data importer have encrypted the data transferred, in such a manner that the US authorities will not be able to decrypt. EU data protection law remains applicable (encryption being a security measure only), including therefore the EU transfer rules. Here the SCCs are an appropriate instrument to ensure an adequate level of protection. A similar conclusion is justified in cases where the data transferred are not sensitive and not of interest to the US authorities (as evidenced e.g. by the limited numbers of subpoenas received by the data importer). Here the SCCs can provide for the adequate protections as envisaged by Article 26(2) Directive. The assessment by the CJEU should be whether in general, the SCCs adduce adequate safeguards rather than whether the SCCs in the most extreme cases (like where the US authorities target such company) the SCCs would provide all required safeguards. Again, any other interpretation would lead to the current systems of derogations for data transfers to non-adequate countries under the Directive having no function. Transfers would then only be possible to countries providing an adequate protection, which is contrary to the legislative history of the Directive.

**Examples** where SCCs provide for additional protections that address the shortcomings of the Safe Harbor system as identified by the CJEU, and for which such additional protections should be taken into account by national DPAs assessing specific transfers under Article 4 of the SCCs:

- **US government access.** SCCs do not provide for any specific exceptions for sharing with governments or law enforcement agencies outside the EU (as the Safe Harbor Decision did, see Schrems, para. 82, as cited in Section 9). Rather SCCs require the data importer to promptly notify the data exporter of any legally binding request for disclosure by a law enforcement authority (unless otherwise prohibited), which enables and entitles the data exporter to suspend the transfer of data and/or terminate the contract. The data importer is further required to deal promptly and properly with all inquiries from the data exporter and to abide by the advice of the supervisory authority with regard to the relevant processing.\(^49\)

- **Oversight, compliance monitoring and jurisdiction.** The CJEU held that the Safe Harbor Decision does not “refer to the existence of effective legal protection against interference” by US government and further that “procedures before the Federal Trade Commission (…) are limited to commercial disputes (…) and the private dispute

\(^{49}\) Clause 5(d) and (e) of SCCs under Decision 2010/87/EU.
resolution mechanisms concern compliance by the United States undertakings with the safe Harbor principles and cannot be applied in disputes relating to the legality of interference with fundamental rights that results from measures originating from the State.” (Schrems, para. 88 and 89).

In contrast, compliance with SCCs is entrusted to the DPAs themselves, and such compliance is reviewed under EU law. Furthermore, in some EU member states SCCs are subject to prior approval by the national DPA, which means that national DPAs have the opportunity to conduct an ex ante review of transfers based on SCCs whereas no such approval was required for transfers based on Safe Harbor.

- **Insufficient Judicial Redress.** The CJEU relied on Commission Communications (COM (2013) 846 final and COM (2013) 847 final) according to which individuals have “no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased” (Schrems para. 90, cited in Section 9).

In contrast, SCCs provide for a right of action for individuals before EEA courts and/or DPAs. Whereas Safe Harbor does not explicitly guarantee third party rights for individuals, SCCs give individuals the right to also obtain compensation for any damages they have suffered.

**BCR**

In Section 15, it was previously noted that BCR are both broader and more limited in scope than adequacy decisions; broader as they may cover transfers to all countries, and more limited as BCR cover transfers by a specific company only (rather than covering all transfers to a country). Thus, the assessment by the lead DPA as to whether BCR can be authorized under Article 26(2) of the Directive as adducing adequate safeguards should not be based on specific assessments of transfers to specific countries, but should be a general assessment of whether BCR meet the criteria set by the WP29 (and by the EU regulators in the GDPR) in respect of BCR. This general assessment must be distinguished from the assessment by DPAs, upon hearing a claim, as to whether specific transfers under specific BCR should be prohibited or suspended based on the powers conferred upon the DPAs under Article 28 of the Directive. In other words, it is possible that BCR receive an EU authorization under Article 26(2) of the Directive as adding adequate safeguards in general (as they indeed do, see examples below), while specific transfers under BCR are suspended by a DPA based on a case-by-case assessment (similar to the one under Article 4 of the SCCs).

---

50 See, inter alia, Clauses 8 and 9 of SCCs under Decision 2010/87/EU, Section IV of Decision 2004/915/EC.
51 There are requirements for prior DPA approval of SCCs in Austria, Belgium, Croatia, Cyprus, Estonia, France, Hungary, Latvia, Lithuania, Luxembourg, Malta, Portugal (for transfers of non-sensitive data only), Romania, Slovenia, and Spain.
52 See Clause 7 of SCCs under Commission Decision 2010/87/EU and Section III of SCCs under Decision 2004/915/EC.
53 Article 6 of SCCs under Commission Decision 2010/87/EU and Section III of SCCs under Decision 2004/915/EC.
It is further possible (as with SCCs), that the laws of a country are not considered adequate for reasons of too extensive government access powers and lack of redress for individuals, while DPAs, upon hearing a claim, come to the conclusion that the specific transfers to such country under BCR are allowed because, in the specific case, there is no substantial adverse impact on individuals. Such specific assessment, however, should not be part of the assessment to be made by a national DPA in the general authorization procedure of BCRs under Article 26(2) of the Directive. Recent statements by certain national DPAs that they will no longer authorize BCR under Article 26(2) of the Directive are therefore unfounded.⁵⁴

Examples where BCR provide for additional protections that address the shortcomings of the Safe Harbor system as identified by the CJEU, and which additional protections should be taken into account by national DPAs making their assessment in respect of specific transfers under BCR (similar to an assessment under Article 4 of the SCCs):

- **U.S. government access.** BCRs for Controllers (BCR-C) do not provide for any specific exception for sharing with governments or law enforcement agencies outside the EU (as the Safe Harbor Decision did, see Schrems, para. 82, as cited in Section 9). Rather BCR-C require that where a member of the group has reasons to believe that the legislation applicable to it prevents the company from fulfilling its obligations under the BCR-C and has substantial effect on the guarantees provided by the rules, such member will promptly inform the EU headquarters (except where prohibited by law). In addition, the BCR-C require that where there is conflict between national law and the commitments in the BCR-C, the EU headquarters will take a responsible decision on what action to take and will consult with the competent DPA in case of doubt.⁵⁵

BCR for Processors (BCR-P) require that where a member of the processors’ group has reasons to believe that legislation applicable to it may prevent it from fulfilling the instructions received from the controller, or its obligations under the BCR or the service agreement, it will promptly notify this to both the controller and the DPA competent for the controller.⁵⁶ BCR-P further require that a specific procedure be implemented for dealing with requests for disclosure of personal data by a law enforcement authority or state security body, which requires the processor to (i) assess each access request on a case-by-case basis as to whether it is valid and binding, (ii) to inform the controller and the lead DPA for the BCR-P of any legally binding Disclosure Requests, unless otherwise prohibited; (iii) to commit to putting the request on hold for a reasonable delay in order to notify the DPA competent for the controller and the lead DPA for the BCR-P prior to the disclosure to the requesting body; (iv) to

---


⁵⁵ See WP 74, section 3.3.3.

⁵⁶ See WP 204, section 2.3.4.
use its best efforts to obtain the right to waive a prohibition to disclose; and (v) in any event provide to the competent DPA general information on the requests it received to the competent DPAs (e.g., number of applications for disclosure, type of data requested, requester if possible, etc.).

- **Oversight, compliance monitoring and jurisdiction.** As with SCCs, compliance with BCR is entrusted to the DPAs themselves, and such compliance is reviewed under EU law. Furthermore, BCR are subject to prior approval by the lead DPA, which means that such lead DPAs and the relevant co-leads, have the opportunity to conduct an *ex ante* review of transfers based on BCR, whereas no such approval was required for transfers based on Safe Harbor.

- **Insufficient Judicial Redress.** BCR-C require an internal complaints handling process, which enables individuals to file a complaint against the group company in their own country. BCR-C and BCR-P further provide for the possibility for individuals to lodge a complaint before the competent DPAs and before the EU courts.

6. **Conclusions**

The analysis shows a number of things.

In the first place, there is the importance of the distinction whether a derogation allowing data transfers to a third country is based on Article 25 Directive or Article 26 Directive, respectively. The adequacy decisions of the Commission based on Article 25 Directive are of a completely different nature than the decisions of the Commission or national DPAs based on Article 26 Directive, authorizing alternative data transfer instruments. In the first case, the Commission evaluates whether the legal regime of the country of destination is adequate, as a result whereof data transfers can take place without implementing additional contractual safeguards. In the second case, the Commission/DPA evaluates whether a set of contractual measures/BCR provide for sufficient safeguards in case the legal regime of the country of destination is not adequate. These concern different assessments based on different criteria. The CJEU observations in the *Schrems* judgment concerning the ‘adequacy’ of US law are therefore not relevant for an assessment of data transfers under the alternative data transfer instruments.

Secondly, the *Schrems* judgment confirms that only the CJEU – and not national DPAs or courts – can strike down a derogation under Article 26. As a consequence, the SCCs and BCR remain valid. Recent blanket statements by certain national DPAs that these transfer instruments are no longer valid for data transfers to the US are therefore legally unfounded. The Irish DPA therefore follows the right route, by not declaring the SCCs invalid for data transfers to the US, but by

---

57 See WP 204 section 2.3.4
58 See n. 36
59 See WP 74, Section 5.6 and WP 204, Sections 4.3 and 4.7.
60 *Schrems*, paragraph 61.
referring the decision to declare the SCCs invalid for data transfers to the US to the Irish court, which in its turn will refer the case to the CJEU.

Thirdly, when assessing the validity of the SCCs as a data transfer tool to the US, the CJEU cannot base its judgment solely on the fact that the redress mechanisms for individuals in the US are not adequate (as the Irish DPA does). The CJEU will have to evaluate whether the SCCs will offer sufficient safeguards so transfers can take place to the US, assuming e.g. the redress mechanisms are not adequate. This is a different assessment than the Irish DPA seems to have made. Further the ECJ will have to take in to consideration any undertakings given by the U.S. government under the Privacy Shield as these also apply to transfers under SCCs (and BCR). Any other interpretation would lead to the current systems of derogations for data transfers to non-adequate countries under the Directive having no function. Transfers would then only be possible to countries providing an adequate protection, which is contrary to the legislative history of the Directive (and the upcoming GDPR for that matter).

Fourthly, national DPAs remain at all times authorized, when hearing a claim, to examine the relevant specific data transfers. This requires a case-by-case assessment considering all relevant circumstances. The ‘adequacy’ of the laws of the country of destination is one factor only and can in itself not be the basis for deciding that the transfers under SCCs or BCR should be prohibited or suspended.

Finally, the EU data transfer rules are based on the fundamental starting point that data transfers may take place to countries that provide a level of protection of fundamental rights that is essentially equivalent to that guaranteed in the EU legal order. It is therefore not appropriate to hold the US to higher standards than we live up to ourselves. Given the discussions on the scope and validity of the surveillance powers and redress of EU citizens in respect thereof, it seems unjustified to require certain standards from the US if there is no clarity in the EU what those standards should be. Similar concerns further raise in respect of the redress mechanisms available in many other countries outside the EU, including other major trading partners of the EU, such as China, Russia, Japan, South Korea, India, Brazil and Canada. Applying inconsistent and discriminatory rules would likely violate the EU’s international trade commitments.

Whatever the standard may ultimately turn out to be, in any event it is by now clear that unbridled data transfers to non-adequate countries is subject to risks and will remain so for quite some time. As a result we see a clear trend to store data in European clouds and further to encrypt data as much as possible without the cloud provider having access to the data (‘bring your own encryption’), to prevent that data can be read when accessed by US or any third country government.

---

61 See n 13.
62 Which measures then trigger the debate whether regulation is necessary to prohibit encryption above a certain level (in order to ensure that government can remain capable to decrypt data) as well as discussions with providers of handheld devices to implement backdoors making it possible for governmental authorities to decrypt the data. See the recent discussion between
Apple and US government, whereby Apple refuses to adapt the iPhone to facilitate decryption of messages, see ‘£120 high street device can unlock an iPhone within hours’, The Telegraph, 4 April 2016: http://www.telegraph.co.uk/technology/2016/04/04/120-high-street-device-can-unlock-an-iphone-within-hours).