Case Note – *Schrems II decision*: An Extra-territorial Approach to Privacy Protection

ELIZABETH REED*

I THE FREE FLOW OF DATA BETWEEN JURISDICTIONS

Data has become an increasingly important part of the world's economy and will only grow in importance as more of the world becomes digital.[1] Having an open, efficient, and transparent flow of data is important for the continued stability of the digital economy. However, the European Union's (EU) enactment of the *General Data Protection Regulation* ('*GDPR*') highlights a tension between the open sharing of data and the need to safeguard individual privacy. The *GDPR* requires that transfers of an EU citizen's personal data to a third country must comply with the regulation to 'ensure that the level of protection guaranteed by the regulation is not undermined'.[2] This requirement restricts the free flow of data between jurisdictions.

The *Schrems II judgment* was a much-anticipated decision of the Court of Justice of the European Union ('CJEU').[3] Referred to the CJEU from the High Court of Ireland, it is the first decision since the enactment of the *GDPR* to consider the transfer of data between the European Union ('EU') and a third country. The CJEU's finding that the EU-US *Privacy Shield Decision* is invalid highlights the significant global reach of the *GDPR*.

This case note will demonstrate how the *GDPR's* extra-territorial nature is shaping the global approach to data privacy protection. Since the *GDPR* requires third countries to meet an 'equivalent level' of privacy protection in order to receive personal data transfers from within the EU, it is necessary to consider whether privacy protection mechanisms provided by the *GDPR* undermine state sovereignty by effectively forcing third countries to adopt laws in line with the *GDPR* rules to obtain 'adequacy decisions', such as the *Privacy Shield Decision*.

---

*BA/LLB (Hons in Law) candidate (University of Tasmania). Co-editor of the *University of Tasmania Law Review* 2020. I am grateful for the supervision of Dr Heather Ann Forrest. All errors remain my own.

[1] Julie Brill, 'Strengthening International Ties Can Support Increased Convergence of Privacy Regimes' 2(2) *European Data Protection Law Review* (2016) 151.

[2] *Regulation (EU) No 2016/679 of the European Parliament and of the Council of the 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)* [2016] OJ 119/ 1 art 44 ('*GDPR*').

[3] *Data Protection Commissioner v Facebook Ireland, Maximillian Schrem, and intervening parties* (Court of Justice of the European union, C-311/18, 16 July 2020) ('*Schrems II*').

II THE CASE

This case is a companion decision to *Schrems I*, which considered a request from Mr Schrems, an Austrian national, to the Data Protection Commission (Ireland) to suspend or prohibit the transfer of his personal data to the United States (US). Upon registering for Facebook, Mr Schrems was required to enter into a contract with Facebook Ireland, which is a subsidiary company of the United States company Facebook Inc.[4] The personal data of Facebook Ireland's users is transferred to Facebook Inc's servers located in the US, where it is processed. Personal data is defined in the *GDPR* as 'any information relating to an identified or identifiable natural person'.[5] A person will be identifiable if they can be identified by reference to an identifier, such as a name.[6] The core of Mr Schrems' complaint was that the US did not 'ensure adequate protection of personal data' held in the US against the surveillance activities of law enforcement authorities.[7] This complaint was rejected by the Ireland Data Protection Commission on the basis of a previous adequacy decision by the European Commission that the US provided an adequate level of protection through what was known as the 'Safe Harbour Framework'.[8] On judicial review, the Irish High Court referred the issue to the CJEU for a preliminary ruling. The CJEU held that the Safe Harbour Framework was invalid, and the High Court subsequently annulled the Commission's rejection of Mr Schrems' complaint.[9] The Ireland Data Protection Commission's investigation following this ruling found that the transfer of data from Facebook Ireland to Facebook Inc is pursuant to the standard data protection clauses in the *Standard Contract Clauses Decision* ('*SCC Decision*').[10] The *SCC Decision* provides that personal data transferred in accordance with the standard contractual clauses ('SCCs') ensure that there are adequate safeguards for the protection of privacy and fundamental rights.[11]

The *Schrems II decision* concerned a subsequently reformulated complaint by Mr Schrems to the Commission. This complaint claimed that US law, in particular s 702 of the *Foreign Surveillance Act* and Executive Order 12333, requires that Facebook Inc make available personal data transferred to it to US law enforcement authorities, such as the National Security Agency ('NSA') and the Federal Bureau of Investigation ('FBI'). Mr Schrems claimed that the data was subject to various monitoring programs

---

[4] Ibid [50]–[51].
[5] *GDPR* (n 2) art 4(1).
[6] Ibid.
[7] *Schrems II* (n 3) [52].
[8] Ibid [52]; Beata A Safari, 'Intangible Privacy Rights: How Europe's GDPR will set a New Global Standard for Personal Data Protection' 47(3) *Seton Hall Law Review* (2017) 809, 813.
[9] *Maximillian Schrems v Data Protection Commissioner, Digital Rights Ireland, Ltd* (Court of Justice of the European Union, C-326/14, 6 October 2015) ('*Schrems I*').
[10] *Schrems II* (n 3) [54].
[11] Ibid [27].

in a manner not compatible with arts 7, 8, and 47 of the *Charter of Fundamental Rights of the European Union* (the '*Charter*').[12] He argued that, given the interference by government authorities, the *SCC Decision* cannot justify the transfer of personal data.[13] In response, Facebook Ireland argued that the *Privacy Shield Decision* was binding on supervisory authorities, such as national data protection commissions, in the context of a transfer of personal data pursuant to the *SCC Decision*. Therefore, in Schrems II, the CJEU considered the validity of both the *SCC Decision* and the *Privacy Shield Decision*.

III Transfers to Third Countries

Article 44 of the *GDPR* requires that data transfers from within the EU to a third country comply with the conditions found in Chapter V of the *GDPR*.[14] Chapter V details different circumstances in which a transfer to outside the EU may take place. Relevant to this case note are article 45, transfers on the basis of an adequacy decision, and article 46, transfers subject to appropriate safeguards.[15]

An adequacy decision means that the European Commission has evaluated the level of protection offered by a third country and has found that the country in question offers an adequate level of protection.[16] If a transfer is made on the basis of an adequacy decision, there is no need to seek any other authorisation.[17] This case focuses on the adequacy decision referred to as the *Privacy Shield Decision*, which allows transfers between the EU and the US. An adequacy decision is the most convenient mechanism for allowing the free flow of data. Without an adequacy decision, controllers must rely on another transfer mechanism, such as SCCs.[18]

The SCCs are one of the appropriate safeguards found in article 46 of the *GDPR*. They are standard contract clauses that have been adopted by a supervisory authority and approved by the European Commission.[19] Appropriate safeguards, such as the SCCs, allow transfers to a third country if the controller or processor has provided appropriate safeguards, the data subject has enforceable rights, and legal remedies are available.[20]

The above mechanisms are important for reducing the commercial and administrative burdens on data controllers who regularly transfer data to

---

[12] *Charter of Fundamental Rights of the European Union* [2012] OJ C 326/391, arts 7, 8, 47.
[13] *Schrems II* (n 3) [55].
[14] *GDPR* (n 2) art 44.
[15] Ibid arts 45, 46(2)(c).
[16] Ibid art 45(1).
[17] Ibid.
[18] *GDPR* (n 2) art 46(2).
[19] Ibid art 46(2)(d).
[20] Ibid art 46(1).

third countries. In addition, they ensure that data subjects have sufficient legal recourse if their personal data is used in a manner contrary to the *GDPR* outside of the EU.

A *Standard Contract Clauses*

One of the key issues raised in the *Schrems II* dispute was whether the use of the standard contract clauses, in accordance with the *SCC Decision*, complies with the terms of the *GDPR*, despite the fact that they only create a contractual obligation between the parties to the contract and, importantly, do not bind US authorities.[21] The *SCC Decision* notably differs from an adequacy decision of the European Commission, as it does not require the European Commission to assess the level of protection assured by third countries.[22] Therefore, the court considered whether, in absence of an adequacy decision, the transfer of personal data pursuant to the *SCC Decision* provides appropriate safeguards to ensure an adequate level of protection equivalent to the protection guaranteed under EU law.[23]

The contractual obligations set out in the *SCC Decision* requires that controllers and recipients provide appropriate safeguards for the data subject's privacy.[24] The court held that the purpose of the SCCs was to provide uniform guarantees that could be applied in all third countries to controllers and processors established in the EU. They can be used regardless of whether the third country offers an adequate level of protection. However, relying on art 46(1) and recitals 108 and 114 of the *GDPR*, in instances where the third country does not have sufficient safeguards, the controller should adopt further supplementary measures.[25] In addition, if the recipient of the personal data is no longer able to fulfill their obligations under the SCCs due to domestic law, then they are required to notify the controller of their inability to comply with the SCCs. In turn, the controller or supervisory body is obliged to suspend the transfer and/or terminate the contract.[26]

Overall, in the absence of an adequacy decision, the court held that the *SCC Decision* provides an effective mechanism for ensuring an adequate level of protection of an EU citizen's personal data. A benefit of the SCCs is that they do not require a third country to change their laws and practices in order for controllers to transfer personal data to the country. This limits the extra-territorial nature of the *GDPR*, to the extent that third countries are not required to offer the equivalent level protection as the EU. Rather, the

[21] *Schrems II*, (n 3) [123].
[22] Ibid [130].
[23] Ibid [105].
[24] Ibid [131].
[25] Ibid [131]–[132].
[26] Ibid [142].

data subject's privacy is protected through the contractual obligations placed on the controller and recipient of the personal data.

B *Privacy Shield Decision*

Since the *Schrems I* decision, the EU and US have negotiated a new agreement for the transfer of personal data between the countries.[27] The *Privacy Shield Decision* allows the free transfer of data to companies that are certified in the US under the Privacy Shield.[28] It was intended to address the shortcomings of the original Safe Harbour Framework by having stronger enforcement measures, greater responsibilities on controllers transferring data, clearer security measures in relation to and more transparency of, US government access, and competent and adequate protection of EU citizens' rights.[29]

1 *Limitations on interference*

The CJEU considered the validity of the *Privacy Shield Decision*, in terms of whether it complied with the *GDPR* when read in light of the *Charter*,[30] in particular, articles 7 and 8, which provide for the respect for private and family life, and for the protection of personal data.[31] These *Charter* rights are not absolute and must be examined in context of their function within society, but any interference with these rights must be limited to what is reasonably necessary to achieve a legitimate goal.[32] The *Privacy Shield Decision* outlines privacy principles, representations and commitments of the US that ensures an adequate level of data protection. However, the decision also provides that privacy principles may be limited to the extent necessary for national security, public interest or law enforcement requirements.[33] Where any of these concerns apply, US data recipients are required to disregard the privacy principles of the Privacy Shield, enabling US authorities to interfere with personal data transferred from the EU.[34]

The CJEU decision considered whether there were sufficient limitations placed on the powers conferred to the US authorities to monitor personal data. It found that the Privacy Shield provides that any interference with personal data by US authorities 'will be limited to what is strictly necessary to achieve the legitimate objective in question, and that exists effective

---

[27] 'EU-US data transfers' *European Commission* (Webpage) <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en>.
[28] *Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, art 1(3).
[29] Safari (n 8) 818.
[30] *Schrems II* (n 3) [161].
[31] *Charter of Fundamental Rights of the European Union* (n 10) arts 7, 8.
[32] *GDPR* (n 2) [172].
[33] *Schrems II* (n 3) [164].
[34] Ibid.

legal protection against such interference'.[35] However, the CJEU held that the US fails to detail the rules for governing the scope of the interference and does not impose minimum safeguards.[36] Further, the powers of US authorities to monitor personal data are limited by Presidential Policy Directive 28, which prescribes the actions taken by US authorities in relation to overseas surveillance.[37] However, the Directive does not grant data subjects enforceable rights and the exercise of the power is not subject to judicial review. Therefore, the Privacy Shield cannot ensure an equivalent level of protection to that which is provided under EU law.

2 *Avenue for Legal Redress*

The court also raised a particular concern that the Privacy Shield did not contain effective legal redress for data subjects whose personal data has been transferred.[38] The Privacy Shield, in response to the finding of invalidity of the Safe Harbour Framework, introduced the Privacy Shield Ombudsperson mechanism. However, the court found that the Ombudsperson is not an independent review mechanism for two reasons. First, the Ombudsperson is appointed and reports directly to the Secretary of State and is considered an 'integral part of the US State Department'.[39] Second, there is nothing to protect the Ombudsperson against dismissal or revocation. These factors undermine this mechanism's ability to be an independent and impartial avenue of redress.[40] Furthermore, the Ombudsperson does not have the power to adopt decisions that are binding on US authorities, thus significantly reducing the level of protection offered to data subjects.

IV Global Implications: Meeting the Standard of the *GDPR*

The decision of the CJEU in *Schrems II* highlights how third countries are expected to meet the level of privacy protection guaranteed by the EU through the *GDPR* and the *Charter*. The invalidation of the *Privacy Shield Decision* is the second time that the CJEU has struck down an adequacy decision between EU and US, which suggests that it is not sufficient for the European Commission and the executive government of a third country to negotiate safeguards relating to the protection of personal data. Rather, countries who wish to benefit from an adequacy decision will need to examine their current laws and practices to ensure that they offer the equivalent level of protection as the EU. This decision emphasises that particular attention needs to be paid to the following: that the processing of

[35] Ibid [167].
[36] Ibid [176].
[37] Ibid [48].
[38] Ibid [188]–[189].
[39] Ibid [195].
[40] Ibid.

personal data is done in accordance with a specific and limited purpose,[41] that EU data subjects are able to have standing to enforce their rights through judicial review, and that any mechanism of administrative oversight is independent from the executive and has the power to adopt binding decisions.[42]

Currently, an adequacy decision is the most efficient means of ensuring that data can freely flow between jurisdictions; an adequacy decision allows the transfer of data without further authorisation or safeguards being needed.[43] While there are benefits to ensuring that countries meet the standard of protection offered by the EU as it encourages uniformity and consistency for the protection of personal information, it also raises concerns that the *GDPR* places obligations on third countries that they have not consented to. Countries wishing to benefit from an adequacy decision are pressured to design their own privacy laws to meet the standard of the EU, thus diminishing the freedom of countries to decide their own regulations.

Short of an adequacy decision between the EU and a third country, greater importance is placed on other means of legally transferring data from the EU to a third country. While it is possible to transfer data pursuant to appropriate safeguards, such as the consent of the data subject, authorisation of a supervisory body, or via SCCs,[44] this places a commercial and administrative burden on controllers to ensure that each transfer to a third country complies with the *GDPR*. With each jurisdiction having vastly different requirements to protect privacy and personal data, there is the potential that this causes inefficiency and undermines the free flow of data. However, as noted by the CJEU, the purpose of the SCCs is to create a uniform approach for controllers to use and rely upon. Furthermore, the SCCs do not require countries to meet EU's standard of protection as they do not require them to change laws and practices, rather controllers are only required to include supplementary measures in instances where countries do not offer an adequate level of protection.

Without an adequacy decision, a greater burden is placed on data controllers and processors to ensure that their transfers to a third country are in accordance with both the *GDPR* and the *Charter*. SCCs offer an effective and uniform method of complying with the *GDPR*, however, the controllers and processers will need to assess on a case-by-case basis whether the protection offered by a third country undermines the efficiency of data transfers between the EU and third countries. This may have further

[41] *Schrems II* (n 3) [173].
[42] Ibid [104] and [196].
[43] *GDPR* (n 2) art 45(1).
[44] Ibid art 46(2).

impacts on the development of the digital economy as trade is increasingly done via the Internet.

V Conclusion

The EU's imposition of a high standard of data and privacy protection ensures EU citizens have enforceable rights against controllers and processors who use their personal data in contrary to the *GDPR*. One of the key strengths of the *GDPR* is that it ensures that this high level of protection extends beyond the EU, accounting for the full use of data by controllers and processors. The benefit of this approach, in terms of the protection of privacy, is that controllers and processors cannot escape liability by moving data to a jurisdiction with a lower level of protection. However, requiring third countries to have the equivalent level of protection as the EU, places increased pressure on third countries to meet the EU's standard of protection which may diminish their regulatory freedom.