The Implications of the *Schrems* Decision and ending of the US-EU Safe Harbour Agreement

Introduction

This article looks at the Court of Justice of the European Union's (CJEU) decision in *Schrems v Data Protestation Commissioner*[1] that was delivered 6th October 2015. This case centres on the transfer of personal data from the EU and its Member States to the US under the Safe Harbour Agreements. This agreement was introduced to enable a freer flow of personal data for trade and industry purposes. However following the revelations of the US' National Security Agency's use of bulk data collection that included accessing the personal data of EU citizens, an Austrian citizen brought his case before the CJEU claiming the NSA would have probably accessed his data held by the social media company Facebook. This article examines what legal factors led to the CJEU making the decision that has resulted in the ending of the Safe harbour Agreement and why it is important that third countries who the EU has agreements have in place adequate legal provisions regarding data protection

The Safe Harbour Agreement

To protect EU citizens' personal data the EU-US Safe Harbour agreement was signed in 2000 under Decision 2000/520/EC in order to provide a streamlined process for US companies to comply with the EU's Data Protection Directive.[2] Among the privacy principles in the agreement it states that organisations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.[3] If US organisations flout EU privacy law the EU Commission can reverse the

[1] [2015] EUECJ C-362/14
[2] Actually termed the European Parliament and Council Directive 95/46/EC
[3] Annex I, paragraph 12 Dec 2000/520, Export.gov, US-EU Safe Harbor Overview at http://www.export.gov/safeharbor/eu/eg_main_018476.asp [accessed 23rd September 2015]

decision to grant the Safe Harbour arrangement.[4] The agreement was mainly aimed at the private sector's access to personal data for business purposes, but in November 2013 the European Commission expressed concerns over the large scale access by US Intelligence agencies to data transferred by Safe-Harbour certified companies.[5] This concern came from the disclosure and revelations by former employee of the US intelligence agency, National Security Agency (NSA), Edward Snowden that the NSA was involved in bulk data collection.[6] This led to the European Commission stressing the importance of the national security exception in the Safe-Harbour Decision should only be used when it is, '…strictly necessary or proportionate'.[7]

How *Schrems* ended the Safe Harbour Agreement

Maximillian Schrems, an Austrian citizen, used the social media network, Facebook, since 2008. Although his contract was registered within the EU at the time of his registration with Facebook Ireland, this is a subsidiary of Facebook Incorporated which is established in the US, where Facebook Ireland users' personal data is then transferred to the US. Schrems contended that the law and practice in the US did not ensure sufficient protection of his personal data and in referring to the Snowden revelations of NSA practices, he claimed his personal data could have been subject to retention by the NSA and other US federal agencies.[8] Perceiving Schrems' complaint as unsustainable in law and bound to fail because he saw it as vexatious, the Irish Data Protection Commissioner did not see himself as being required to investigate the complaint as there was no evidence that Schrems' personal data

[4]Art 3(4) Dec 2000/520European Commission, How will 'safe harbor' arrangement for personal data transfer to the US work? (09/10/2012) at http://ec.europa.eu/justice/policies/privacy/thridcountries/adequacy-faq1_en.htm [accessed 23rd September 2015]
[5] European Commission, Communication on the Functioning of the Safe-Harbour from the Perspectives of EU Citizens and Companies Established in the US, COM(2013)847 Final, p.18
[6] G. Greenwald, No Place to Hide: Edward Snowden, the NSA and the US Surveillance State (2014 New York: Metropolitan Books) p.92
[7] Dec 2000/520, p.19
[8] Ibid, paragraphs [26] – [30]

had been accessed by the NSA.[9] In Schrems' judicial review of the Irish Commissioner's decision,[10] the Irish High Court held once personal data has been transferred to the US it is capable of being accessed by the NSA and other US federal agencies in the course of indiscriminate surveillance and interception of communications.[11] Justice Hogan said if this matter was to be measured solely by Irish law and Irish constitutional standards a serious issue would arise which the Commissioner would have been required to investigate whether US law and practice in relation to privacy, interception and surveillance matched those standards.[12] Acknowledging the Snowden revelations had exposed 'gaping holes' in contemporary US data protection practice,[13] Justice Hogan did not see Schrems complaints as 'frivolous or vexatious'[14]and refereed it to the CJEU.

In the Opinion of the Advocate General, Advocate General Bot held that as intervention of independent supervisory authorities is at the heart of the EU's system of personal data protection, there must be a similar system of protection in the third country to which the data flows from the EU.[15] In this case under the US' surveillance Act, Foreign Intelligence Surveillance Act 1978, the NSA accessed personal data inputted in Austria that was held by Facebook at a server in the US, Advocate General Bot held that the Foreign Intelligence Surveillance Court does not offer an effective judicial remedy to EU citizens whose personal data has been transferred to the US.[16] He proposed that when the case went to the CJEU it should answer the question if the agreement is invalid.[17] The CJEU did answer this question

[9] *Maximillian Schrems v Data Protection Commissioner* Case C-362/14 (Advocate General Opinion - delivered 23rd September 2015), paragraph [30]
[10] *Maximillian Schrems v Data Protection Commissioner* [2014] IEHC 310
[11] Ibid, paragraph [14]
[12] Ibid, paragraph [79]
[13] Ibid, paragraph[69]
[14] Ibid, paragraph [74]
[15] n 9, paragraph [210]
[16] Ibid, at [210] and [211]
[17] Ibid, at [237]

and declared the 2000/520 Decision as invalid[18] and consequently brought to an end the Safe Harbour Agreement. Crucial to the Court reaching this decision were the requirements of article 25 of the 95/46 Directive on data protection. Where communications data is transferred from outside the EU to a third country, the EU is responsible for ensuring the third country has an adequate level of data protection. In doing so, consideration is given to the nature of the data, the purpose and duration of the processing operation of the data, the country of origin and final country of destination, the law in operation related to data protection in the third country and the professional rules and security measures deployed regarding the data in the third country.[19]

The most pertinent part of article 25 related to the issue in *Schrems* is it being the Commission's responsibility to find that the third country ensures an adequate level of protection of basic freedoms and rights of individuals.[20] Should the Commission find the third country does not provide an adequate level of protection, Member States are to take measures to prevent the transfer of data to the third country.[21] Crucial to determining this is what is meant by the term 'adequate'. The third country is not required to ensure there is a level of data protection identical to that guaranteed in EU law,[22] Advocate General Bot said that the protection implemented by the third country may differ from EU law, but it must provide adequate protection that is equivalent to that afforded by the 95/46 Directive.[23] Adopting the linguistic viewpoint of the word 'adequate' which means satisfactory or sufficient, Advocate General Bot said the obligation of the Commission is to ensure the third country has a sufficiently high level of protection of fundamental rights.[24] The obligation to

[18] n 1, paragraph [107]
[19] art 25(2) Directive 95/46/EC
[20] Ibid, art 25(6)
[21] Ibid, art 25(4)
[22] n 1, paragraph [73]
[23] n 9, paragraph [141]
[24] Ibid, paragraph [142]

ensure the adequacy of data protection is not a one-off obligation made at the time of agreement. The obligation for the third country is an ongoing obligation to ensure that no changes in circumstances arise that can call into question the initial assessment[25] and it is expected the Commission will regularly review the third country's level of protection.[26] It was on this legal point that Schrems was successful as the CJEU found the 2000 Decision did not cover the situation to limit interference by US state bodies authorised under legitimate objectives, such as national security, in US law to interfere with personal data transferred from the EU.[27] The Court added that legislation permitting public authorities access to the content of electronic communications on a *generalised basis* must be regarded as compromising the essence of the fundamental right to privacy under the CFRF.[28] This echoes the CJEU's decision in *Digital Rights*[29] where an authority for a state agency to access communications data must be specific with a legitimate aim along with sufficient safeguards protecting potential abuse by a state agency's use of that data. On the latter point, in *Schrems* the CJEU found there to be no effective remedy for an individual ensure the data was used in compliance with legal provisions similar to those found in the EU.[30]

The main surprise from cases like *Schrems* is not in finding that the Safe Harbour Agreement was ruled as invalid it is that this Agreement lasted for fifteen years. Supporting this point, there is no single authority dedicated to overseeing data protection law in the US, as Sotto and Simpson observe, the US legislative framework designed to protect personal data resembles a 'patchwork quilt'.[31] As the US favours commercial enterprises, personal

[25] Ibid, paragraph [147]
[26] Ibid, paragraph [137], n6, paragraph [76]
[27] n 1, paragraph [88]
[28] Ibid, paragraph [94]
[29] [2014]EUECJ C-293/12, [2014] 3 WLR 1607
[30] Ibid, paragraph [95]
[31] L.J. Sotto, and A.P. Simpson, 'United States' in R.P. Jay (editor), Data Protection & Privacy in 26 jurisdictions worldwide 2014, (London: Law Business Research, 2014), 191, p.191

data is largely regulated by trade associations.[32] Although the US' Federal Trade Commission (FTC) oversees the provisions of the agreement regarding consumer privacy issues, including the collection and use of personal information, with an authority to do so under section 5 FTC Act[33] it is only in relation to unfair acts or practices affecting commerce. The Safe Harbour Agreement only required US companies to develop their own self-regulatory privacy policies to conform with the EU's data protection principles to qualify them for Safe Harbour[34] rather than adherence to a federal law providing greater safeguards. The problem with self-certification is it lends personal data open to potential abuse. These are the gaping holes Justice Hogan referred to when Schrems was at the Irish High Court. Potential abuse was found by the EU in their first two reviews of Safe Harbour that raised significant concerns. The 2002 review found a substantial number of organisations that signed up to self-certified adherence were not observing the expected degree of transparency regarding the contents of their privacy policies and in the 2004 review it was found that less than half of the organisations signed up to the Agreement reflected observance of all seven Safe Harbour principles.[35] As this Agreement was set up to facilitate a freer movement of data in relation to international trade could explain why some of these points were overlooked. While there is an argument for self-regulation due its lower burden on business and trade,[36] the weakness of Safe Harbour is that EU citizens' personal data was transferred to a jurisdiction with fewer privacy protections leaving that data vulnerable to access and abuse by US federal agencies like the NSA. Following the Snowden revelations the US and the EU have been negotiating an update to Safe Harbour since 2013 with the EU looking to limit the circumstances US

[32] A. Muir and C. Oppenheim 'National Information Policy developments worldwide IV: copyright, freedom of Information and data protection' (2002) Journal of Information Science (28) 467, 478
[33] Annex V Dec2000/520
[34] Ibid Annex I, paragraph 3
[35] C. Connelly, 'The US Safe Harbor – Fact or Fiction?'(Galexia Pty Ltd 2008), at paragraph 2
[36] D.Haynes, 'End of Safe Harbour isn't the end of the world – let's hope its successor is better', The Conversation 12th October 2015, at http://theconversation.com/end-of-safe-harbour-isnt-the-end-of-the-world-lets-hope-its-successor-is-better-48841 [accessed13th October 2015]

federal agencies could access the transferred data. Even though the US was set to agreeing to this, US politicians may retaliate against the *Schrems* decision by refusing to grant the privilege.[37] However, transnational business and trade needs may overcome politicians' petulance and a new Safe Harbour Agreement will be signed in the near future containing greater legal safeguards regarding data protection that is more truly equivalent those contained with the 95/46 Directive.

It may come as a surprise that the US has no legislation that deeply embeds data protection within its legal system. Other western states that have agreements with the EU appear to apply similar legal principles in relation to data protection. For example the US' northern neighbour, Canada has the Privacy Act 1985 as well as Personal Information Protection and Electronic Documents Act 2000, the latter being concerned solely with the use of electronically stored personal data. Both Acts are clear that personal information cannot be used unless it meets strict criteria[38] similar to the provisions in the 95/46 Directive and both Acts also have sufficient safeguards where individuals can make complaints to the Privacy Commissioner[39] and the Canadian courts.[40] Likewise the Australia's Privacy Act 1988 contains similar provisions as the Canadian legislation with section 7 promoting the privacy of an individual's personal data with the safeguards including complaints to the Australian Privacy Commissioner[41] or to an Australian Court.[42] As both Canada and Australia have agreements with the EU regarding the processing and transfer of passenger name record data held by air carriers[43] the two respective states' legislation clearly offers a level of protection

[37] L. Kelion, 'Facebook data transfers threatened by Safe Harbour ruling' BBC News 6th October 2015, at http://www.bbc.co.uk/news/technology-34442618 [accessed 6th October 2015]
[38] s.7 Privacy Act (1985 (Canada), s.4 Personal Information Protection and Electronic Documents Act 2000 (Canada)
[39] Ibid, s.29, s.11
[40] Ibid, s.34, s.46
[41] s. 34 Privacy Act 1988 (Australia)
[42] Ibid, s.46
[43] Agreement (Canada) L 82/15, Agreement Australia L 186/4

equivalent to that afforded by the 95/46 Directive. The decisions in *Digital Rights* and *Schrems* demonstrates how EU law views the importance in protecting personal data and why it is best placed as an international actor to encourage those third countries it has agreements with to adopt similar measure in relation to data protection.

Conclusion

The CJEU's decision in *Schrems* that ended the Safe-Harbour agreement between the EU-US was a courageous move by the Court on two counts. Firstly the CJEU knew the implications of ending the Agreement would have in relation to business and financial institutions effectiveness to operate on both sides of the Atlantic Ocean. The second being through the CJEU, the EU was not deterred in aggravating one of the most politically and economically powerful states, the US as the *Schrems* decision is a strong slap in the face of US data protection law, or should I say its lack of data protection law. *Schrems* is not the EU seeking revenge on the US following the revelations of the NSA's abuse in the collection and use of communications data related to EU citizens, this decision was made to ensure future agreements operate under the rule of law reassuring citizens the activities of intelligence and policing agencies operate on a sound legal footing. As we now live in the age of transnational companies and financial institutions having operating centres and district headquarters in various states throughout the world, the transfer of personal data is one of the crucial components in oiling the wheels of industry. It is vital that any third county where personal data is transferred from an EU Member State has adequate legal protection and safeguards in relation to personal data, especially where it can be accessed by that third country's state agencies. There will be a successor to the EU-US Safe Harbour agreements, but one where personal data will have a greater degree of protection because the message Schrems gives out is if you wish to do business with the EU and its Member States you have to make sure you take data protection seriously.