The Future of Transatlantic Data Transfer Following the Invalidation of the Safe Harbour Agreement

In 2015, the European Court of Justice ruled that the Safe Harbour agreement is invalid[1]. The Safe Harbour agreement was introduced in 2000[2] to bridge the differences in data protection law within the United States of America (US) and the European Union (EU). Specifically, it laid out principles that US organisations could adhere to in order to store and process personal data on EU citizens. These principles within Safe Harbour guided US organisations towards accepting EU law on data protection. Within the EU, all member states must implement data protection legislation as directed by the Data Protection Directive that was introduced in 1995[3]. Article 25 of the Data Protection Directive states explicitly that the transfer of personal data to countries outside the EU may only take place if the countries in question ensure sufficient levels of data protection, in line with that of the EU, by reason of domestic laws or international commitments. Conversely, the US has never formally introduced any legislation on data protection[4]. Hence, before Safe Harbour, if personal data originally held in Europe was transferred to the US, there was potential for legal conflict. It was this problem of EU to US data transfer that initially inspired the creation of Safe Harbour. So, why did the European Court of Justice decide to invalidate the Safe Harbour principles in 2015, after 15 years of agreement? Furthermore, what are the implications of this decision?

The origin of the Safe Harbour decision can be traced to the case of Maximillian Schrems against the Irish Data Protection Commissioner. In 2013, Schrems filed a complaint against Facebook, stating that his personal data provided to Facebook's servers located in Ireland was not sufficiently protected once transferred to servers located in the US[1]. Schrems cited the revelations revealed by Edward Snowden in 2013[5] as evidence that the law and practice of the US did not offer adequate protection of his data from mass surveillance, and claimed that his fundamental right to privacy and data protection would be violated under the Safe Harbour agreement. Initially, the Irish Data Protection Authority rejected the complaint because the US did offer adequate protection under Safe Harbour[6]. However, after oral hearings concerning the validity of Safe Harbour[7], the European Court of Justice ruled that the Safe Harbour agreement is invalid[1] on the 6th of October 2015.

The Court found the agreement to be invalid because the agreement itself does not refer to the public authorities of the US, rather it solely refers to individual organisations[1]. Hence, personal data on EU citizens could be legally processed with the aim of fulfilling American national security and law enforcement without adhering to the requirements of EU privacy law. This observation completely conflicts with the objectives that Safe Harbour was initially created to accomplish. The Court also found that there were no judicial means in which EU citizens could access, modify or delete data once that data had entered the US, this breaches a fundamental principle within the Data Protection Directive[8]. For these reasons, the European Court of Justice stated that the Safe Harbour agreement alone could no longer legitimise the transfer of personal data from the EU to the US.

One of the major implications of this decision is the demand for a replacement or change to Safe Harbour that meets the criteria of the EU[9], [10]. In the aftermath of the decision, the legal uncertainty of data transferral over the Atlantic has enhanced. However, there are clear reasons to resolve this quickly. The US-EU economic relationship is the largest in the world[8], made up of online commerce trade avenues worth over $1 trillion. These trade avenues are very much enabled by data flows between the EU and the US. In light of these facts, both the EU and the US agreed on a new framework called the EU-US Privacy Shield early in February 2016 to replace Safe Harbour[11], in order to swiftly avoid costly bureaucracy. The EU revealed that with the new Privacy Shield, the US had given the EU assurance that it will subject limitations onto the US public authorities regarding the personal data of European citizens. Subsequently, the Vice President of the European Commission for the Digital Single Market, Andrus Ansip stated: "Our people can be sure that their data is fully protected"[11].

However, there has not been total consensus over the content of the new framework. Maximillian Schrems highlighted that there is still no mechanism in which individual EU citizens can lodge

complaints about the use of their data or the transparency scheme that is supposed to ensure the lack of involvement from US intelligence agencies[12]. Schrems is referring to the newly instated role of an ombudsperson in the Privacy Shield. Although the ombudsperson is independent of public authorities and is responsible for handling complaints, the EU-US Privacy Shield guide states that a complaint's response from the ombudsperson will not reveal any involvement of surveillance from US national intelligence services[13]. As a result, the Privacy Shield will still not inform European citizens of U.S. surveillance. Delving further on this matter, the European Data Protection Supervisor, Giovanni Buttarelli, stated that "the Privacy Shield, as it stands, is not robust enough to withstand future legal scrutiny before the [European] Court"[14]. Also, the executive director of European Digital Rights Joe McNamee criticised the timing of the political agreement providing the foundations for the EU-US Privacy Shield, stating that the European Commission had announced the agreement too soon, effectively decreasing the negotiation period they could have utilised to further the privacy agenda[15]. Although McNamee has highlighted the downside of a short negotiation period, a very long negotiation period can also have displeasing consequences, specifically for EU citizens. Mass surveillance, as revealed by Edward Snowden, could still occur on EU citizens' personal data during a long transition window in data protection legislation, as US authorities would still be able to process data without consequence, hence prolonging the problem identified with Safe Harbour.

The decision also has significant implications for companies and businesses throughout the EU and the US who previously relied on Safe Harbour to conduct transatlantic data transfer. While there is no robust replacement for Safe Harbour, many EU businesses that use US companies for data storage or data processing could be in breach of the EU Data Protection Directive. They must now find alternative means to achieve the same goal[16]. Similarly, US companies operating in the EU can no longer transfer data back to their servers located in the US. Large and established companies could afford to build data centres and store data in Europe to counteract the problem. However, smaller startups that cannot afford to construct substantial infrastructure would have to temporarily halt their European branches of business, which could prove to be time-consuming and very costly[17].

To avoid making these adjustments, companies on both sides of the Atlantic can avoid the data transfer problem by signing 'model contracts' and implementing 'binding corporate rules' with EU authorities[18]. Binding corporate rules allow international companies to perform intra-organisational data flow from the EU to the rest of the world[19]. Model contracts contain specific clauses dictating the methods of data transfer from the EU to the rest of the world[20]. These instruments can achieve transatlantic data flow in the absence of Safe Harbour. However, model contracts and binding corporate rules could prove costly for both companies and the EU. Companies must devote funds and time to drafting legal documents in order to prove acceptance of EU standards, which could significantly impact the productivity of small and large organisations. Also, the EU must decide whether or not to accept contracts with every individual company separately. As time moves on and the number of companies increases, this method would quickly become infeasible and too time-consuming for the EU.

The initial motivation behind the Safe Harbour agreement was to bridge the gaps in EU and US legislation on data protection while promoting transatlantic data transfer. While model contracts and binding corporate rules can allow transatlantic data flow, they cannot represent a formal agreement between the EU and the US on data protection. Following the invalidation of Safe Harbour, a replacement agreement between the EU and the US must be put in place, because the privacy of EU citizens must be kept intact (as laid out in EU privacy law) and the economic value of transatlantic trade underpinned by data should not be diminished. Although the EU-US Privacy Shield has been labelled as a worthy replacement, it is simply not robust enough to stand the test of time. The Privacy Shield is still subject to legal scrutiny from privacy activists[14], which could lead to yet another invalidation decision and more uncertainty. Significant time must be taken to construct a new agreement between the US and the EU. Even though an extended transition period may undermine EU citizens' personal data in the short term, future privacy breaches may be prevented by a thoroughly negotiated US-EU agreement. Concerning the content of a new agreement, there should be new frameworks put in place that can allow EU citizens to observe and alter their personal data directly. Furthermore, there should be thorough negotiation concerning the methods used to gather intelligence. After all, the heart of the Safe Harbour invalidation decision was the privacy issue raised by Edward Snowden in which mass surveillance

was shown to be practised within the US. Once a new agreement is in place, companies will need to dedicate funds and time to adhere to it. Although, in return, EU citizens will be able to entrust their personal data to organisations and businesses, thus promoting economic growth, and promoting the very objective that the Safe Harbour agreement was initially created to achieve.

References:

1. Court of Justice of the European Union. (October, 2015). PRESS RELEASE No 117/15: Judgment in Case C-362/14: Maximillian Schrems v Data Protection Commissioner. Retrieved from https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf. Accessed on 01/12/2017.

2. European Commission. (July, 2000). 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.). Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000D0520&from=EN. Accessed on 01/12/2017.

3. European Parliament. (October, 1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML. Accessed on 01/12/2017.

4. Jolly, Ieuan. (July, 2017). Data Protection in the United States: Overview. Retrieved from https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1. Accessed on 01/12/2017.

5. MacAskill, Ewen and Dance, Gabriel. (November, 2013). NSA Files: Decoded, What the revelations mean for you. Retrieved from https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1. Accessed on 01/12/2017.

6. RTE. (July, 2013). Data Protection Commissioner says no action will be taken against Apple and Facebook. Retrieved from https://www.rte.ie/news/2013/0726/464770-data-protection/. Accessed on 01/12/2017.

7. Lachtnain, Antoin. (March, 2015). Revelations on Safe Harbour Violations Go to Hearing at EU Court. Retrieved from http://delano.lu/news/revelations-safe-harbour-violations-go-hearing-eu-court. Accessed on 01/12/2017.

8. Meltzer, Joshua P. (November, 2015). Examining the EU Safe Harbour Decision and Impacts for Transatlantic Data Flows. Retrieved from https://www.brookings.edu/testimonies/examining-the-eu-safe-harbor-decision-and-impacts-for-transatlantic-data-flows/. Accessed on 01/12/2017.

9. Office of Public Affairs. (October, 2015). Statement from U.S. Secretary of Commerce Penny Pritzker on European Court of Justice Safe Harbor Framework Decision. Retrieved from https://www.commerce.gov/news/press-releases/2015/10/statement-us-secretary-commerce-penny-pritzker-european-court-justice. Accessed on 01/12/2017.

10. Weiss, Martin A. and Archick, Kristin. (May, 2016). U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield. Congressional Research Service. Page 8. Retrieved from https://epic.org/crs/R44257.pdf. Accessed on 01/12/2017.

11. European Commission. (February, 2016). Press Release: EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield. Retrieved from http://europa.eu/rapid/press-release_IP-16-216_en.htm. Accessed on 01/12/2017.

12. Meyer, David. (July, 2016). This Facebook Nemesis Says Businesses Will Shun U.S.-EU Privacy Deal. Retrieved from http://fortune.com/2016/07/11/schrems-privacy-shield/. Accessed on 01/12/2017.

13. European Commission. (2016). Guide to the EU-U.S. Privacy Shield. Pages 19-20. Retrieved from http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_en.pdf. Accessed on 01/12/2017.

14. European Data Protection Supervisor. (May, 2016). Press Release EDPS/2016/11: Privacy Shield: more robust and sustainable solution needed. Retrieved from https://edps.europa.eu/sites/edp/files/edpsweb_press_releases/edps-2016-11-privacyshield_en.pdf. Accessed on 01/12/2017.

15. McNamee, Joe. (February, 2016). What's behind the shield? Unspinning the "privacy shield" spin. Retrieved from https://edri.org/privacyshield-unspinning-the-spin/. Accessed on 01/12/2017.

16. Gibbs, Samuel. (October, 2015). What is 'safe harbour' and why did the EUCJ just declare it invalid? Retrieved from https://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection. Accessed on 01/12/2017.

17. Kharpal, Arjun. (October, 2015). US and EU in data privacy clash: What you need to know. Retrieved from https://www.cnbc.com/2015/10/07/eu-safe-harbor-ruling-what-is-it-and-what-does-it-mean-for-us-tech-firms.html. Accessed on 01/12/2017.

18. Mortera-Martinez, Camino and Korteweg, Rem. (November, 2015). Adrift: The Impact of the ECJ's Safe Harbour Ruling. Centre for European Reform. Retrieved from http://www.cer.eu/sites/default/files/bulletin_105_cmm_rk_article2.pdf. Accessed on 01/12/2017.

19. International Commissioner's Office. (2017). Binding Corporate Rules. Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/binding-corporate-rules/. Accessed on 01/12/2017.

20. International Commissioner's Office. (2017). Model Contract Clauses. Retrieved from https://ico.org.uk/media/1571/model_contract_clauses_international_transfers_of_personal_data.pdf. Accessed on 01/12/2017.