EU-US Safe Harbour Invalidation and its Implications

EU privacy laws forbid sending its citizens' private data outside of the European Union, except when the location where the information is received has privacy laws in line with the EU ones. In 2000, a Safe Harbour framework (The Data Protection Directive 95/94/EC) has been established between the United States of America and the European Union, allowing US companies to send data from their European offices across the Atlantic Ocean under certain circumstances (6), but this was ruled invalid by the European Court of Justice on 6 October 2015 due to a two-year old case submitted by an Austrian privacy campaigner, Maximillian Schrems (1). The reason why Mr. Schrems complained was that his Facebook private data was being sent from Facebook Irish' subsidiary to the Facebook headquarters in US and the privacy laws in the United States did not ensure that his data was no subject to surveillance from American authorities. As he stated in the file, “in the light of the revelations made in 2013 by [Edward Snowden](https://en.wikipedia.org/wiki/Edward_Snowden) concerning the activities of the [United States intelligence services](https://en.wikipedia.org/wiki/United_States_Intelligence_Community) (in particular the [National Security Agency](https://en.wikipedia.org/wiki/National_Security_Agency) (‘the NSA’)), the law and practice of the United States do not offer sufficient protection against surveillance by the public authorities”. Its implications are not only heavily affecting US companies, which cannot have a free movement of data among their offices, but also us, as EU citizens, and our data privacy. However, a new agreement was reached on 2 February 2016 called “EU-US Privacy Shield” that promises positive prospects for all involved parties (2).

Before considering the invalidation's implications, it is important to note and understand why this event occurred. In 2000, when The Data Protection Directive was promulgated, Internet was not as widely spread as it is today (7), thus the regulations and main principles behind the Safe Harbour scheme became questionable nowadays. The agreements were considered invalid on 23 September 2015 by General Advocate Yves Bot on the grounds that national supervisory authorities should have full power and rights to stop any transfer of data that they find questionable, therefore having the ability to rule against any decision made by the Commission (8). This was the case with Maximillian Schrems, a Facebook user since 2008, who, after Edward Snowden's leaks in 2013, thought that his private data might be under surveillance by US bodies (e.g. NSA) as they were sent from Facebook's Irish subsidiary to American servers. He lodged a complaint to the Irish supervisory authority which rejected it on the grounds that the Commission issued a directive in 2000 stating that if a third party is considered to have adequate privacy laws, data can be freely moved (1). This complaint was sent further to the High Court of Ireland, which wanted to ascertain if a national supervisory authority has the right to question if the third country ensures adequate levels of protection (i.e. United States of America). The General Advocate's decision was accepted by the European Court of Justice on 6 October 2015, the main reasons being: compromising the right to respect for private life, compromising the actual right to judicial protection and, finally, that the Commission had no right to restrict the national supervisory authority, in Mr. Schrems' case the Data Protection Commissioner (1). Therefore, the Harbour Scheme Decision was oficially declared invalid.

The vast majority of people do not want their private data to be used or manipulated by any other party, including governments or federal bodies. In studies conducted by several institutions (e.g. Eurobarometer – 2011, IIPS – 2008, Deloitte - 2012) (5), 59 to 84% of the people interviewed said that disclosing personal information, such as financial, health details or ­even social media activity, is a big issue. Therefore, one of the main positive aspects of the Safe Harbour agreements' invalidation was the increase of privacy for EU citizens' data and the awareness among people regarding how vulnerable their personal data is. As Internet is becoming a primordial part of our daily lives, the amount of data we share online is increasing dramatically and, without proper protection, we are subject to possible misuse or even espionage. In 2013, Edward Snowden leaked more than 1.7 million NSA classified documents, showing the world the degree of surveillance we are facing. After this event occurred, as awareness started to increase, people became more eager to protect themselves against privacy invasion and complained to different authorities both in US and EU, among which the above-mentioned Mr. Schrems succeeded in making the ECJ rule against the Safe Harbour agreements. On the other hand, as such a large number of companies is affected by this ruling, users might face problems while using various websites and online resources until everything is rethought. For these reasons, we are expecting more regulations and better constructed legal frameworks that will protect the users' data in much more secure ways.

Having considered the EU citizens' point of view, is is providential to look at the tremendous effects on both EU and US businesses. Previously, around 6000 American companies relied on the Safe Harbour scheme to legally move data out of the European area (ultima). Having this framework invalidated, it will have a big impact on both large companies and start-ups until various alternatives are found. Even though The Internet Association stated that most big companies have other means of transferring data legally, a very large number of start-ups relied primarily on Safe Harbour and they will need to rethink their whole business process, being put on hold until further agreements between the 2 parties (9). Furthermore, there is not only a need for alternatives, but there will be dramatic economical effects: in an anonymous survey conducted by DMA with smaller and bigger companies from both Europe and UK-only (e.g. Barclays, Sky) , 16% said that they will suffer losses between £50.000 and £100.000, while 63% will be deprived of less than £10.000. Exposing these arguments, companies, as mentioned before, have different alternatives to apply until an agreement is reached between the EU and the US, 2 of which being: Model Contract Clauses, that is adequate safeguards to protecting the privacy and fundamental rights of an individual (14) and Binding Corporate Rules, meaning internal rules for multi-national companies defining their global policies around legal and thorough international transfer of data (15).

The last point we need to take into consideration is the ongoing struggle to find the best alternative to the Safe Harbour framework. On 2 February 2016, the “EU-US Privacy Shield” took shape, which is a new framework developed jointly by the United States and the European Union implying strong obligations and enforcement for businesses' transferring European citizens' private data, transparency on US government access to such information, as well as a better system for protecting the citizens' fundamental rights (16). A very small number of companies has adopted this new framework yet, but it is expected that it will be embraced at a larger scale, mostly by companies who relied heavily on the defunct Safe Harbour. Despite this option, there are criticisms not only from a number of law experts, but also from the person whose case made the initial framework invalid, Maximillian Schrems. He stated that all European citizens will still be subject to surveillance from US authorities, as long as this is legal on the other side of the Atlantic (17). ------------ de adaugat aici --------------

In the final analysis, it can be concluded that the invalidation of the Safe Harbour framework was correct judgement from the European Court of Justice. The principles behind it were outdated due to the immense Internet traffic and data sharing we are facing today and the users will benefit from enhanced privacy and a sense of security. Moreover, the level of awareness among people Edward Snowden created with leaking the classified documents and Max Schrems fighting for privacy rights with Facebook and eventually ruling against a 15-year old law is beneficial for our understanding of personal data and how rights regarding our personal online data can be violated. However, as the new EU-US Privacy Shield that should replace and improve the previous scheme has just come out, very few companies have adopted it and we are still not sure how this will evolve. Further observations need to be made and a conclusion needs to be taken if the new law will protect our data flows and fundamental rights as EU citizens.

Sources

1-

["Judgment in Case C-362/14 Maximillian Schrems v Data Protection Commissioner: The Court of Justice declares that the Commission’s US Safe Harbour Decision is invalid"](http://curia.europa.eu/jcms/jcms/P_180250/) (press release) (Press release). Court of Justice of the European Union. 6 October 2015. p. 3. Retrieved 29 February 2016.

2 -

[EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield](http://europa.eu/rapid/press-release_IP-16-216_en.htm), issued 2 February 2016

3 -

Chris Strohm and Del Quentin Wilber (January 10, 2014). ["Pentagon Says Snowden Took Most U.S. Secrets Ever: Rogers"](http://www.bloomberg.com/news/2014-01-09/pentagon-finds-snowden-took-1-7-million-files-rogers-says.html). [Bloomberg News](https://en.wikipedia.org/wiki/Bloomberg_News). Retrieved February 1, 2014.

4 -

<http://www.computerweekly.com/news/4500254944/EU-Safe-Harbour-ruling-requires-a-rethink-of-data-processes>, [Warwick Ashford](http://www.techtarget.com/contributor/Warwick-Ashford), [06 Oct 2015 17:30](http://www.computerweekly.com/news/4500254944/EU-Safe-Harbour-ruling-requires-a-rethink-of-data-processes)

5 -

<http://www.sciencewise-erc.org.uk/cms/assets/Uploads/SocialIntelligenceBigData.pdf>

6 -

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>

7 -

<http://www.dekunder.nl/Media/10.1007_s11192-016-1863-z.pdf>

8 -

<http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-09/cp150106en.pdf>

9 -

<http://www.olswang.com/articles/2015/09/data-transfers-to-the-us-safe-harbor-declared-invalid-what-are-your-options-now/>

10 -

[https://en.wikipedia.org/wiki/International\_Safe\_Harbor\_Privacy\_Principles#cite\_note-inval-10](https://en.wikipedia.org/wiki/International_Safe_Harbor_Privacy_Principles" \l "cite_note-inval-10)

11 -

<http://www.cnbc.com/2015/10/07/eu-safe-harbor-ruling-what-is-it-and-what-does-it-mean-for-us-tech-firms.html>

12 -

<https://safeharbor.export.gov/list.aspx>

13 -

<http://www.dma.org.uk/uploads/ckeditor/pdfs/Safe_Harbour_results_(inc_exec_summary).pdf>

14 -

<http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm>

15 -

<http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm>

16 -

<http://europa.eu/rapid/press-release_IP-16-216_en.htm>

17 -

http://www.bbc.co.uk/news/technology-35471851